Analisis Risiko Keamanan Data pada Platform Cloud Computing

Habib Risky Kurniawan[1*],Irfan Nur Sofiyanto[2],Muhammad Faqih Habiburrohman[3]

[1]*Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta [1*]220103178@mhs.udb.ac.id (penulis korespondensi)*

[1]*Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta [1*]220103178@mhs.udb.ac.id (penulis korespondensi)*

[1]*Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta [1*]220103178@mhs.udb.ac.id (penulis korespondensi)*

Abstrak— **Dalam beberapa tahun terakhir, berbagai organisasi di Indonesia telah mengadopsi komputasi awan (cloud computing). Meskipun teknologi ini menawarkan banyak manfaat, seperti skalabilitas, pengurangan biaya, dan fleksibilitas, adopsi teknologi ini juga disertai dengan masalah besar terkait keamanan data. Keamanan data platform cloud computing adalah subjek penelitian ini, Kami menemukan berbagai ancaman keamanan, seperti serangan siber, kebocoran data, dan kerentanan sistem, melalui penelitian literatur yang menyeluruh dan analisis studi kasus pada beberapa perusahaan. Kami juga mengevaluasi teknologi dan praktik terbaik untuk meningkatkan keamanan data serta peran penyedia layanan cloud dalam menjaga keamanan data pengguna. Penelitian ini memberikan wawasan mendalam tentang ancaman keamanan data pada paltform komputasi awan dan menawarkan saran praktis bagi organisasi untuk mengelola risiko tersebut. Oleh karena itu, diharapkan penelitian ini dapat membantu para pengambil keputusan dalam penerapan solusi komputasi awan yang aman dan dapat diandalkan.**

Kata kunci— Keamanan Data, Cloud Computing, Risiko Keamanan, Serangan Siber, Enkripsi Data

Abstract— **In recent years, various organizations in Indonesia have adopted cloud computing. Although this technology offers many benefits, such as scalability, cost reduction, and flexibility, its adoption also comes with significant data security issues. Data security on cloud computing platforms is the subject of several companies, we found various security threats, such as cyber-attacks, data breaches, and system vulnerabilities. We also evaluated technologies and best practices to enhance data security, as well as the role of cloud service providers in safeguarding user data. This research providers in-depth insights into data security threats on cloud computing platforms and offers practical recommendations for organizations to manage these risks. Therefore, it is expected that this research will assist decision-makers in implementing secure and reliable cloud computing solutions.**

Keywords— Keamanan Data, Cloud Computing, Security Risks, Cyber-Attacks, Data Encryption.

I. PENDAHULUAN

Komputasi Awan adalah suatu teknologi yang menjadikan internet sebagai pusat server untuk mengelola data dan informasi[1]. Beberapa tahun terakhir, Komputasi Awan (cloud computing) semakin banyak diadopsi oleh berbagai organisasi di Indonesia[2]. Komputasi awan menawarkan banyak manfaat akses data mencakup pengurangan biaya, fleksibilitas, skalabilitas, pengurangan masalah operasional, dan potensi investasi jangka panjang[3]. Namun, manfaat ini juga disertai dengan risiko keamanan data yang harus dipertimbangkan dengan cermat.

Keamanan data pada platform cloud computing menjadi isu kritis karena data yang disimpan dan diproses di sistem cloud rentan terhadap berbagai bahaya, termasuk serangan dunia maya, pelanggaran data, dan pelanggaran privasi[4]. Selain itu, mengandalkan pengelolaan dan penyimpanan data pihak ketiga mempersulit proses memastikan keamanan dan kerahasiaan data[5]. Oleh karena itu, penggunaan layanan skomputasi awan memerlukan tingkat kepercayaan yang tinggi untuk mengkomunikasikan informasi pribadi[6].

Ancaman keamanan data komputasi awan dapat berdampak besar pada bisnis, mulai dari hilangnya data penting hingga pelanggaran undang-undang privasi data dan pembayaran denda yang besar[7]. Oleh karena itu, untuk membantu perusahaan dalam menerapkan langkah-langkah pencegahan dan mitigasi yang diperlukan, kesadaran menyeluruh terhadap ancaman keamanan data yang terkait dengan platform komputasi awan sangatlah penting.

Tujuan dari penelitian ini adalah untuk mengkaji secara menyeluruh risiko yang terkait dengan keamanan data pada platform komputasi awan. Berbagai jenis ancaman keamanan, seperti serangan siber, kesalahan manusia, dan kelemahan sistem akan diidentifikasi dan dievaluasi[8]. Selain itu, kami akan membahas teknologi yang dapat digunakan untuk meningkatkan keamanan, praktik terbaik untuk mengelola keamanan data di cloud, dan peran

penyedia layanan cloud dalam menjaga keamanan data pengguna.

Dengan adanya analisis ini diharapkan dapat memberikan pemahaman yang lebih menyeluruh mengenai ancaman keamanan data pada platform komputasi awan dan cara-cara yang dapat digunakan oleh dunia usaha untuk menjaga data mereka dengan lebih baik. Selain itu, diharapkan para pengambil keputusan akan menggunakan studi ini sebagai referensi ketika menerapkan solusi komputasi awan yang aman dan dapat diandalkan.

II. METODOLOGI PENELITIAN

1. Studi Literatur

A. Pendahuluan

Pada tahap awal penelitian, kami melakukan studi literatur yang komprehensif untuk mengumpulkan informasi terkini terkait risiko keamanan data pada platform cloud computing. Tinjauan terhadap berbagai sumber, termasuk buku, laporan penelitian, jurnal ilmiah, dan sumber terpercaya lainnya, merupakan bagian dari studi literatur ini. Studi literatur ini membantu dalam memahami berbagai aspek keamanan cloud computing dan memberikan landasan teoritis yang kuat untuk penelitian ini.

B. Keamanan Data pada Cloud Computing

Cloud computing merupakan teknologi yang menawarkan banyak manfaat seperti pengurangan biaya, fleksibilitas, skalabilitas, dan pengurangan masalah operasional[9]. Namun, adopsi teknologi ini juga membawa risiko keamanan yang signifikan. Data yang disimpan dan diproses dalam sistem cloud rentan terhadap berbagai ancaman seperti serangan siber, pelanggaran data, dan pelanggaran privasi[8]. Beberapa penelitian menunjukkan bahwa ancaman keamanan ini dapat berdampak besar pada bisnis, mulai dari hilangnya data penting hingga pelanggaran undang-undang privasi data dan denda yang besar.

C. Ancaman Keamanan pada Cloud Computing

Menurut [10], terdapat 11 ancaman keamanan padacloud computing, yaitu:

1. Pengelolaan Identitas, Kredensial, Akses, dan Kunci yang Tidak Memadai
2. Antarmuka dan API yang Tidak Aman
3. Kesalahan Konfigurasi dan Pengendalian Perubahan yang Tidak Memadai
4. Kurangnya Arsitektur dan Strategi Keamanan Cloud
5. Pengembangan Perangkat Lunak yang Tidak Aman
6. Sumber Daya Pihak Ketiga yang Tidak Aman
7. Kerentanan Sistem
8. Pengungkapan Data Cloud secara Tidak Sengaja
9. Kesalahan Konfigurasi dan Eksploitasi Beban Kerja Serverless dan Container
10. Kejahatan Terorganisir/Hacker/APT
11. Eksfiltrasi Data Penyimpanan Cloud

Selain itu, menurut penelitian [11], kesalahan manusia juga merupakan faktor signifikan yang dapat mengakibatkan pelanggaran keamanan data di cloud. Penelitian ini menyoroti pentingnya pengelolaan keamanan yang baik untuk mencegah kesalahan manusia yang dapat berakibat fatal.

D. Teknologi dan Praktik Terbaik untuk Keamanan Cloud

Berbagai teknologi telah dikembangkan untuk meningkatkan keamanan data pada cloud computing. Misalnya, enkripsi data, autentikasi multi-faktor, dan firewall telah terbukti efektif dalam melindungi data dari akses yang tidak sah. Dalam jurnal [6], menekankan pentingnya penerapan enkripsi data end-to-end dan penggunaan protokol keamanan yang kuat untuk menjaga integritas dan kerahasiaan data di cloud.

E. Peran Penyedia Layanan Cloud

Penyedia layanan cloud memainkan peran kunci dalam menjaga keamanan data pengguna. Dalam penelitian [9], menjelaskan bahwa penyedia layanan cloud harus memastikan bahwa mereka menerapkan kebijakan dan praktik keamanan yang ketat untuk melindungi data pelanggan mereka.

2. Identifikasi Risiko Keamanan

Berdasarkan studi literatur yang telah dilakukan, kami mengidentifikasi berbagai jenis risiko keamanan data yang terkait dengan platform cloud computing. Risiko-risiko tersebut dapat dikategorikan sebagai berikut:

1. Serangan Siber
   a) Serangan Distributed Denial of Service (DDoS)
   b) Serangan injeksi kode berbahaya
   c) Serangan malware dan virus
   d) Eksploitasi kerentanan sistem
   e) Pembajakan akun
2. Kebocoran dan Pencurian Data
   a) Kebocoran data akibat kesalahan konfigurasi
   b) Pencurian data oleh pihak internal yang tidak bertanggung jawab
   c) Akses tidak sah ke data sensitif
   d) Kehilangan perangkat yang berisi data rahasia
3. Kerentanan Sistem dan Infrastruktur Cloud
   a) Kerentanan pada sistem operasi dan aplikasi
   b) Kerentanan pada antarmuka API (*Application Programming Interface*)
   c) Kerentanan pada komponen jaringan
4. Risiko Akses dan Pengendalian
   a) Pengelolaan akses dan hak istimewa yang lemah
   b) Kurangnya pemantauan dan audit aktivitas pengguna
5. Risiko Terkait Penyedia Layanan Cloud
   a) Kebijakan dan perjanjian tingkat layanan yang tidak jelas

3. Studi Kasus

Untuk memperoleh pemahaman yang lebih mendalam tentang risiko keamanan data pada platform cloud computing dan bagaimana organisasi mengelolanya, kami melakukan studi kasus pada beberapa perusahaan yang telah mengadopsi teknologi ini. Studi kasus ini melibatkan wawancara dengan pihak-pihak terkait seperti manajer TI, ahli keamanan, dan pengguna akhir.

1. Studi Kasus 1: Perusahaann Fintech

Perusahaan fintech ini telah menggunakan platform cloud untuk menyimpan dan memproses data keuangan pelanggan. Dalam wawancara, manajer TI perusahaan mengungkapkan bahwa mereka pernah mengalami insiden kebocoran data akibat kesalahan konfigurasi. Insiden ini menimbulkan kekhawatiran besar tentang keamanan data dan memaksa perusahaan untuk meningkatkan kontrol keamanan serta merevisi kebijakan keamanan mereka.

2. Studi Kasus 2: Perusahaan E-commerce

Perusahaan e-commerce ini mengandalkan platform cloud untuk mengelola operasi bisnisnya, termasuk menyimpan data pelanggan dan transaksi penjualan. Dalam wawancara, ahli keamanan perusahaan menyoroti tantangan dalam mengelola akses dan hak istimewa pengguna secara efektif, terutama ketika ada karyawan yang berganti atau berhenti bekerja. Mereka juga menghadapi risiko serangan DDoS yang dapat mengganggu layanan mereka.

3. Studi Kasus 3: Instansi Pemerintah

Sebuah instansi pemerintah telah mengadopsi platform cloud untuk menyimpan dan mengelola data sensitif warga negara. Dalam wawancara, pejabat TI instansi tersebut mengungkapkan kekhawatiran tentang risiko kepatuhan terhadap peraturan privasi data dan standar keamanan yang ketat. Mereka juga

menyoroti tantangan dalam memastikan transparansi praktik keamanan dari penyedia layanan cloud.

4. Analisis Data

Setelah mengumpulkan data dari studi literatur dan studi kasus, kami melakukan analisis mendalam untuk mengidentifikasi pola, tren, dan hubungan antara berbagai jenis risiko keamanan data serta strategi dan praktik terbaik yang dapat diterapkan untuk mengelola risiko tersebut.

Dari analisis data, kami menemukan bahwa serangan siber, seperti DDoS, injeksi kode berbahaya, dan eksploitasi kerentanan sistem, merupakan ancaman yang paling sering dihadapi oleh organisasi yang menggunakan platform cloud computing. Selain itu, kebocoran data akibat kesalahan konfigurasi dan kurangnya pengendalian akses yang memadai juga menjadi masalah yang umum terjadi.

Beberapa tantangan utama yang dihadapi organisasi dalam mengelola keamanan data pada platform cloud computing antara lain:

b) Kurangnya transparansi praktik keamanan dari penyedia layanan cloud
c) Kesulitan dalam memastikan kepatuhan terhadap peraturan privasi data dan standar keamanan
d) Pengelolaan akses dan hak istimewa pengguna yang kompleks
e) Ketergantungan pada penyedia layanan cloud tunggal

Strategi dan praktik terbaik yang dapat diterapkan oleh organisasi untuk mengelola risiko keamanan data pada platform cloud computing, antara lain:

a) Melakukan audit keamanan secara berkala
b) Mengimplementasikan kontrol keamanan teknis dan administratif yang kuat
c) Memberikan pelatihan keamanan kepada karyawan secara teratur
d) Memilih penyedia layanan cloud yang terpercaya dan memenuhi standar keamanan
e) Menerapkan enkripsi data dan manajemen kunci yang tepat
f) Memantau aktivitas pengguna dan melakukan audit trail
g) Menyusun rencana keberlangsungan bisnis dan pemulihan bencana

5. Validasi Temuan

Untuk memastikan keabsahan dan keandalan temuan penelitian, kami melakukan validasi dengan melibatkan bapak Bondan Wahyu Pamekas, S.Kom, M.Kom, seorang pakar di bidang keamanan informasi yang merupakan dosen pengampu mata kuliah tersebut.

Dalam wawancara dengan beliau, kami memaparkan temuan awal penelitian dan meminta masukan serta umpan balik. Beberapa masukan penting yang diperoleh dari validasi dengan dosen keamanan informasi antara lain:

a) Saran untuk memperkuat pembahasan tentang aspek kepatuhan terhadap peraturan dan standar keamanan yang berlaku, seperti GDPR dan ISO 27001.
b) Pentingnya mempertimbangkan risiko keamanan yang spesifik untuk setiap model penyampaian layanan cloud (IaaS, PaaS, SaaS).
c) Masukan untuk memperluas studi kasus dengan melibatkan organisasi dari sektor yang berbeda, seperti pemerintahan, kesehatan, dan keuangan.
d) Saran untuk memperkuat rekomendasi terkait pemantauan dan audit keamanan secara berkala pada lingkungan cloud computing.

Melalui validasi dengan dosen keamanan informasi ini, kami mendapatkan masukan dan umpan balik yang sangat berharga untuk memperkuat dan menyempurnakan temuan penelitian kami.

6. Penyusunan Rekomendasi

Berdasarkan analisis data dan masukan dari proses validasi dengan dosen keamanan informasi, kami menyusun rekomendasi praktis bagi organisasi dalam mengelola risiko keamanan data pada platform cloud computing. Rekomendasi ini mencakup strategi pencegahan, mitigasi, dan pemantauan keamanan yang efektif.

1. Lakukan penilaian risiko keamanan data secara berkala untuk mengidentifikasi potensi ancaman dan kerentanan dalam lingkungan cloud computing.
2. Lakukan evaluasi yang menyeluruh terhadap penyedia layanan cloud yang potensial, termasuk praktik keamanan, transparansi, dan kepatuhan terhadap standar keamanan. Negosiasikan perjanjian tingkat layanan yang jelas dan menguntungkan, terutama terkait aspek keamanan dan privasi data.
3. Terapkan kontrol keamanan teknis seperti enkripsi data, manajemen kunci yang aman, autentikasi multi-faktor, dan pemisahan tugas. Implementasikan juga kontrol keamanan administratif seperti kebijakan keamanan yang ketat, pelatihan karyawan, dan prosedur operasi standar.
4. Lakukan pemantauan keamanan secara berkelanjutan untuk mendeteksi aktivitas mencurigakan dan insiden keamanan. Lakukan audit keamanan secara berkala untuk mengevaluasi efektivitas kontrol keamanan dan mengidentifikasi area yang memerlukan perbaikan.

Pastikan kepatuhan terhadap peraturan dan standar keamanan yang berlaku, seperti GDPR, ISO 27001, dan peraturan industri spesifik. Terapkan mekanisme untuk memastikan kepatuhan secara berkelanjutan dan lakukan pembaruan sesuai dengan perkembangan peraturan dan standar.

III. HASIL DAN PEMBAHASAN

Penelitian ini mengidentifikasi berbagai ancaman dan risiko yang terkait dengan keamanan data pada platform cloud computing. Berdasarkan analisis dari studi literatur, wawancara ahli, dan studi kasus, ditemukan beberapa temuan utama:

1. Jenis ancaman keamanan
   a. Serangan DdoS : Mengganggu layanan yang diberikan oleh platform cloud
   b. Injeksi kode berbahaya : Mengakses atau merusak data yang disimpan di cloud
   c. Eksploitasi kerentanan sistem : Menggunakan kelemahan sistem untuk mendapatkan akses tidak sah
   d. Kesalahan konfigurasi : Konfigurasi yang tidak tepat menyebabkan kebocoran data
   e. Pengelolaan identitas dan akses : Pengelolaan yang tidak memadai dapat menyebabkan akses tidak sah
2. Tantangan dalam mengelola keamanan data
   a. **Transparansi Praktik Keamanan dari Penyedia Layanan Cloud**: Kurangnya informasi mengenai langkah-langkah keamanan yang diambil oleh penyedia layanan cloud
   b. **Kepatuhan terhadap Peraturan dan Standar Keamanan**: Memastikan bahwa data di cloud memenuhi semua peraturan dan standar yang berlaku, seperti GDPR dan ISO 27001
   c. **Pengelolaan Akses dan Hak Istimewa Pengguna**: Kompleksitas dalam mengelola hak akses pengguna, terutama dengan adanya pergantian karyawan
   d. **Ketergantungan pada Penyedia Layanan Cloud Tunggal**: Risiko yang terkait dengan mengandalkan satu penyedia layanan

Berdasarkan temuan tersebut, penelitian ini memberikan beberapa rekomendasi untuk mengelola risiko keamanan data pada platform cloud computing:

1. Audit Keamanan Secara Berkala : Melakukan audit keamanan secara rutin untuk mengidentifikasi dan mengatasi kerentanan yang ada
2. Implementasi kontrol keamanan teknis dan administratif :
   a. Kontrol teknis : Enkripsi data, manajemen kunci yang aman, autentikasi multi-faktor, dan pemisahan tugas
   b. Kontrol administratif : Kebijakan keamanan yang ketat, pelatihan karyawan, dan prosedur operasi standar
3. **Pemantauan dan Audit Trail**: Melakukan pemantauan terus-menerus terhadap aktivitas pengguna dan melakukan audit trail untuk mendeteksi aktivitas mencurigakan dan insiden keamanan
4. **Memilih Penyedia Layanan Cloud yang Terpercaya**: Evaluasi yang menyeluruh terhadap penyedia layanan cloud potensial termasuk praktik keamanan, transparansi, dan kepatuhan terhadap standar keamanan
5. **Enkripsi Data dan Manajemen Kunci yang Tepat**: Mengimplementasikan enkripsi data end-to-end dan menggunakan protokol keamanan yang kuat untuk menjaga integritas dan kerahasiaan data di cloud
6. **Rencana Keberlangsungan Bisnis dan Pemulihan Bencana**: Menyusun rencana keberlangsungan bisnis dan pemulihan bencana untuk memastikan bahwa organisasi dapat terus beroperasi meskipun terjadi insiden keamanan

Dengan menerapkan rekomendasi tersebut, organisasi diharapkan dapat mengelola risiko keamanan data pada platform cloud computing dengan lebih efektif, memastikan bahwa data mereka tetap aman dan sesuai dengan peraturan yang berlaku.

IV. KESIMPULAN

Penelitian ini menyelidiki risiko keamanan data pada platform cloud computing, mengidentifikasi berbagai ancaman keamanan, dan memberikan rekomendasi praktis untuk mengelola risiko tersebut. Berdasarkan studi literatur yang komprehensif dan analisis studi kasus pada beberapa perusahaan, kami mengidentifikasi berbagai risiko keamanan data, termasuk serangan siber, kebocoran dan pencurian data, kerentanan sistem dan infrastruktur cloud, serta risiko terkait akses dan pengendalian. Temuan ini menunjukkan bahwa serangan siber seperti DdoS, injeksi kode berbahaya, dan eksploitasi kerentanan sistem adalah ancaman paling umum, sementara kesalahan konfigurasi dan pengelolaan akses yang tidak memadai sering kali menyebabkan kebocoran data.

Dalam menangani ancaman-ancaman ini, teknologi dan praktik terbaik seperti enkripsi data, autentifikasi multi-faktor, firewall, serta pemantauan dan audit keamanan secara berkala, telah terbukti efektif. Penyedia layanan cloud juga memainkan peran kunci dalam menjaga kemanan data pengguna dengan menerapkan kebijakan dan praktik keamanan yang ketat. Selain itu, studi kasus mengungkapkan tantangan praktis yang dihadapi organisasi dalam mengelola keamanan data di lingkungan cloud, termasuk kurangnya transparansi praktik keamanan dari penyedia layanan cloud, kesulitan memastikan kepatuhan terhadap peraturan privasi data, dan kompleksitas pengelolaan akses pengguna.

Untuk mengelola risiko ini secara efektif, kami merekomendasikan beberapa langkah. Pertama, melakukan penilaian risiko keamanan data secara berkala untuk mengidentifikasi potensi ancaman dan kerentanan. Kedua, melakukan evaluasi menyeluruh terhadap penyedia layanan cloud potensial, termasuk praktik keamanan, transparansi, dan kepatuhan terhadap standar keamanan. Ketiga, menerapkan kontrol keamanan teknis dan administratif yang kuat, seperti enkripsi data, manajemen kunci yang aman, autentikasi multi-faktor, pemisahan tugas, kebijakan keamanan yang ketat, dan pelatihan karyawan. Keempat, melakukan pemantauan keamanan secara berkelanjutan untuk mendeteksi aktivitas mencurigakan dan insiden keamanan, serta

melakukan audit keamanan secara berkala. Kelima, memastikan kepatuhan terhadap peraturan dan standar keamanan yang berlaku, seperti GDPR dan ISO 27001, serta mekanisme untuk memastikan kepatuhan berkelanjutan

Melalui penerapan strategi dan praktik terbaik ini, organisasi dapat meningkatkan perlindungan data mereka di lingkungan cloud, mengurangi risiko keamanan, dan memastika solusi komputasi awan yang aman dan dapat diandalkan.

REFERENSI

[1] P. R. & A. Irawan, "Tinjauan Literatur: Layanan Komputasi Awan Dalam Pengembangan Sistem Pendidikan Perguruan Tinggi," *Researchgate.Net*, no. February, 2023, doi: 10.13140/RG.2.2.16503.50088.

[2] D. David and U. K. Indonesia, "Menuju masa depan komputasi awan: tren infrastuktur dan teknologi baru," no. April, 2024, doi: 10.13140/RG.2.2.19129.99682.

[3] S. Setiawan and A. Gui, "Faktor-Faktor Penentu Yang Mempengaruhi Adopsi Cloud Computing Di Indonesia," *Infotech J. Technol. Inf.*, vol. 9, no. 1, pp. 1–8, 2023, doi: 10.37365/jti.v9i1.144.

[4] E. Suhendar, "Tinjauan Sistematis : Implementasi Cloud Computing Terhadap Keamanan Layanan Publik," *Smart Comp Jurnalnya Orang Pint. Komput.*, vol. 11, no. 4, pp. 599–606, 2022, doi: 10.30591/smartcomp.v11i4.4245.

[5] D. Z. M. Z. M. R. K. Novianti Indah Putri, "Strategi Dan Peningkatan Keamanan Pada Komputasi Awan," *J. Sist. Inf.*, vol. 03, no. 01, pp. 43–50, 2021.

[6] A. Fahrezi, N. Apriliani, N. Ajijah, and D. Juardi, "Keamanan Data dan Transaksi dalam Pemanfaatan Cloud sebagai Service," *J. Pendidik. dan Konseling*, vol. 4, no. 4, pp. 5530–5536, 2022.

[7] B. J. P. Lumbanbatu, "Keamanan Dan Privasi Dalam Sistem Cloud Computing: Tantangan Dan Solusi," *Coursework.Uma.Ac.Id*, pp. 1–13, [Online]. Available: https://coursework.uma.ac.id/index.php/informatika/article/view/1049%0Ahttps://coursework.uma.ac.id/index.php/informatika/article/view/1049/835

[8] M. I. P. N. Suhada, "Keamanan Dan Privasi Data Dalam Lingkungan CloudComputing: Tantangan Dan Solusi," *KOHESI J. Sains Dan Teknol.*, vol. Volume 01, no. 10, pp. 71–80, 2023.

[9] A. Wijoyo, A. R. Silalahi, A. Raihan, P. Arrasyid, and R. Diana, "Sistem Informasi Manajemen Berbasis Cloud," vol. 1, no. 2, pp. 1–15, 2023.

[10] S. and R. Conference, "Cloud Security Alliance's Top Threats to Cloud Computing: Pandemic 11 Report Finds Traditional Cloud Security Issues Becoming Less Concerning," *CSA Official Press Release*, 2022. https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning

[11] Arfan Dwi Madya, Bagas Djoko Haryanto, and Devi Putri Ningsih, "Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 127–135, 2023, doi: 10.60076/indotech.v1i3.236.