SEMINAR NASIONAL TEKNOKA

Vol. 8, 2023
ISSN No. 2502-8782

Analisis Dampak Cloud Computing terhadap Keamanan Sistem dan Data

Razman Rifany[1)], Mario Dwi Prakoso[2)], Pandu Dwi Laksono[3)]
Teknik Informatika, Fakultas Teknologi Industri dan Informatika, Universitas Muhammadiyah Prof. Dr. Hamka Jl. Tanah Merdeka No.6, Pasar Rebo, Jakarta Timur Telp:021-8778.2739
Website: https://ft.uhamka.ac.id/, E-mail: Razmanrifany@uhamka.ac.id, Pandu.lembang99@gmail.com, mariodwiprakoso@gmail.com

Abstrak

Penelitian ini berfokus pada dampak cloud computing. Metodologi penelitian yang dilakukan ini yaitu dengan Literatur secara sistematis, studi kasus, analisis data dan kajian teoritis dengan tujuan untuk pengumpulkan data yang mendukung dalam penelitian dan mencari referensi penelitian yang sama untuk memaksimalkan dalam penelian, serta stategi mitigasi dan pengelolaan risiko yang digunakan. Hasil menunjukkan bahwa dampak penggunaan cloud computing pada keamanan sistem dan integritas data dapat diukur secara konkrit melalui pengujian sumber daya cloud. Penggunaan metode analisis komprehensif membuka wawasan terhadap kelemahan keamanan yang mungkin muncul selama adopsi cloud computing. Penelitian mengidentifikasi tantangan utama, seperti akses tidak sah dan kebocoran data, yang dihadapi oleh pengguna cloud. Hasil survei dan pengujian sumber daya cloud menegaskan perlunya pengembangan kebijakan keamanan yang terfokus, dengan implementasi praktik terbaik sebagai landasan. Langkah pengamanan data yang diberikan adalah dengan melakukan metode autentikasi, metode enkripsi, dan memilih layanan cloud yang dapat di percaya.

Keyword: *Komputasi awan, awan, Sistem Keamanan, Keamanan Awan, AWS*

Abstract

This research focuses on the impact of cloud computing. The research methodology involves systematic literature review, case studies, data analysis, and theoretical examination to collect supportive data and references, aiming to maximize research efficiency. The study also incorporates mitigation strategies and risk management approaches. The findings indicate that the impact of cloud computing on system security and data integrity can be tangibly measured through cloud resource testing. Utilizing comprehensive analytical methods sheds light on security vulnerabilities that may arise during cloud computing adoption. The research identifies key challenges faced by cloud users, such as unauthorized access and data leakage. Survey outcomes and cloud resource testing reinforce the necessity for focused security policy development, emphasizing the implementation of best practices. Data security measures recommended include authentication methods, encryption techniques, and selecting trustworthy cloud services. These security steps serve as safeguards to enhance data protection within the cloud environment.

Kata Kunci*: Cloud Computing, Cloud, Scurity System, Scurity Cloud, AWS*

1. PENDAHULUAN

Revolusi teknologi informasi telah membawa perubahan paradigma dalam cara menyimpan, memproses, dan mengakses data. Di tengah pergeseran ini, konsep Cloud Computing telah menjadi pilar utama yang mengubah cara perusahaan dan individu memanfaatkan teknologi.

Cloud Computing merupakan sebuah model untuk kenyamanan, akses jaringan on-demand untuk menyatukan pengaturan konfigurasi sumber daya komputasi seperti, jaringan, server, media penyimpanan, aplikasi, dan layanan yang dapat dengan cepat ditetapkan dan dirilis dengan usaha manajemen yang minimal atau interaksi dengan penyedia layanan [4].

Cloud computing tidak hanya menawarkan fleksibilitas dan skalabilitas yang luar biasa, tetapi juga memberikan perhatian kriris terhadap keamanan sistem dan data. Perusahaan dan organisasi di seluruh dunia terus berpindah dari infrastruktur lokal ke solusi cloud untuk keunggulan kompetitif dan efisiensi operasional. Namun, sambil mengadopsi teknologi cloud yang inovatif ini, perhatian terhadap kerentanan keamanan juga tumbuh. Tetapi, meskipun Cloud Computing menawarkan kemudahan yang luar biasa, ada satu masalah krusial yang muncul yakni Security Issue. Sifat terbuka dari Cloud Computing, di mana semua orang dapat mengaksesnya, bersamaan dengan sifat internet yang juga terbuka, membuka potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang

Dipresentasikan pada Tanggal 2 Desember 2023

tidak memiliki niat baik. Beberapa orang menggunakan internet untuk tujuan menyerang dan merusak jaringan, yang dapat mengakibatkan penurunan performa atau bahkan lumpuhnya jaringan tersebut [1].

Dalam makalah ini akan melakukan analisis menyeluruh terkait dampak yang yang dihadirkan oleh Cloud Computing terhadap keamanan sistem dan data. Melalui pemahaman yang mendalam, kita akan mengeksplorasi implikasi positif dan negatif dari migrasi ke lingkungan cloud, mengidentifikasi ancaman keamanan yang mungkin timbul, serta mengevaluasi strategi dan solusi untuk melindungi sistem dan data dalam lingkungan yang terhubung secara global ini.

2. LANDASAN TEORI

2.1 Pengertian Analisis

Analisis merupakan proses sistematis untuk merumuskan dan mengorganisir data, menemukan pola, makna, dan implikasi dari informasi yang dikumpulkan. Menurut Rabbani, F. (2008).

2.2 Pengertian Cloud Computing

Cloud computing merujuk pada penggunaan sumber daya komputasi (seperti server, penyimpanan data, basis data, jaringan, perangkat lunak, dan lainnya) yang disediakan melalui internet. Hal ini memungkinkan akses cepat, fleksibilitas, dan penyediaan layanan IT secara on-demand tanpa memerlukan pengelolaan langsung terhadap infrastruktur fisik oleh pengguna. Model ini menawarkan berbagai layanan seperti IaaS (Infrastructure as a Service), PaaS (Platform as a Service), dan SaaS (Software as a Service). Menurut Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A.& Zaharia, M. (2010).

I. Review litrature: Melakukan pencarian jurnal yang terkait dengan keamanan penggunaan cloud computing di berbagai platform seperti Google Scholar. Dilakukan tinjauan secara sistematis dan deskriptif terhadap literatur, mencakup temuan penelitian, teori, dan konsep yang relevan.
II. Studi Kasus: Menemukan contoh-contoh terkait keamanan dalam penggunaan cloud computing untuk penyimpanan data dalam lingkup universitas, organisasi, atau institusi. Tujuannya adalah untuk memberikan gambaran tentang celah-celah keamanan yang mungkin muncul dalam penggunaan cloud computing.
III. Analisis Data: Menghimpun data dari berbagai sumber seperti buku dan jurnal untuk memahami implementasi keamanan Cloud Computing.
IV. Kajian Teoritis: Melakukan analisis teoritis untuk mendukung pemahaman tentang penerapan keamanan Cloud Computing [3].

Berikut tentang tinjauan literatur yang dilakukan dalam membuat makalah ini.

2.3 Pengertian Keamanan Sistem Cloud

Cloud computing: implementation, management, and security. CRC Press. Keamanan sistem di cloud merujuk pada serangkaian praktik, kebijakan, teknologi, dan prosedur yang dirancang untuk melindungi data, infrastruktur, dan layanan yang disimpan, diproses, dan diakses dalam lingkungan cloud. Ini mencakup perlindungan terhadap akses tidak sah, enkripsi data, pengelolaan identitas, deteksi ancaman, pemantauan keamanan, dan kepatuhan terhadap regulasi yang berlaku. Menurut Rittinghouse, J. W., & Ransome, J. F. (2016).

2.4 Pengertian Data

Data adalah sumber daya penting di organisasi yang perlu dikelola seperti mengelola aset penting dalam bisnis lainnya. Saat ini, perusahaan tidak dapat bertahan hidup atau berhasil tanpa data yang berkualitas mengenai operasi internal dan lingkungan eksternal mereka. Data memiliki dasar – dasar konsep data James O'Brien (2013).

3. METODE PENELITIAN

No	*Penulis*	*Tahun*	*Topik*
1	Yuli Fauziah	2014	Tinjauan Keamanan Sistem Pada Teknologi Cloud Computing
2	Mohamed Almorsy, John Grundy, Ingo Müller	2016	An Analysis of the Cloud Computing Security Problem
3	Mohammad Fachry, Ari Kusyanti dan Kasyaful Amron	2018	Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing

ISSN No. 2502-8782

4	Ihsan Taofik, Irawan Afrianto	2023	Analisis Keamanan dan Perlindungan Data pada Komputasi awan dalam ruang lingkup pendidikan
5	Munirul Ula	2019	Analisis Metode Pengamanan Data Pada Layanan Cloud Computing
6	Issac Odun Ayo, Sanjay Misca dan Olasupo Ajayi	2018	Cloud computing security: Issues and developments
7	Mulyana, Irawan Afrianto	2023	Tinjauan Literatur: Analisis Keamanan Sistem Pada Komputasi Awan
8	Nedrick Chandra, Ferry	2023	Cloud Computing ANALISIS ANCAMAN KEAMANAN DATA DALAM CLOUD COMPUTING
9	Satriya, Pratama	2023	PEMANFAATAN TEKNOLOGI SISTEM KOMPUTASI AWAN DALAM PERLINDUNGAN DATA PRIBADI DI INDONESIA
10	Adi Nugroho, Techn Khabib Mustofa	2012	IMPLEMENTASI KOMPUTASI AWAN MENGGUNAKAN TEKNOLOGI GOOGLE APP ENGINE(GAE) DAN AMAZON WEB SERVICES(AWS)

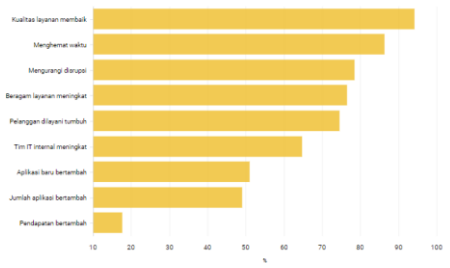
4. HASIL DAN PEMBAHASAN

Dari berbagai penelitian yang telah ditemukan, Cloud computing adalah gabungan pemanfaatan teknologi computer dan pengembangan berbasis cloud storage [7]. Pada cloud computing data informasi tersimpan pada suatu server yang tidak perlu diketahui keberadaannya oleh pengguna, pengguna cukup menikmati fasilitas yang disediakan oleh provider cloud tersebut [7]. Keamanan adalah suatu yang harus di perhatikan dengan teliti terutama keamanan dalam menggunakan cloud computing yang mana layanan tersebut dapat digunakan oleh banyak orang tanpa adanya kriteria sehingga hal tersebut harus menjadi suatu perhatian bahwasannya yang mengakses cloud memiliki tujuan masing-masing yang tidak menutup kemungkinan ada tujuan yang kurang baik [3].

Google dan Amazon telah menjadi pelopor dalam konsep komputasi awan, diikuti oleh Salesforce. Kemudian, perusahaan besar seperti Microsoft, yang menghadirkan Microsoft Azure, turut serta dalam pengembangan ini. Inti dari komputasi awan adalah pusat pemrosesan dan penyimpanan data yang dapat berlokasi di mana saja di dunia ini, memanfaatkan berbagai jenis perangkat mulai dari komputer besar (mainframe), komputer mini, hingga komputer pribadi (PC-Personal Computer). Teknologi pemrosesan yang memungkinkan interaksi antara beragam jenis komputer ini, termasuk sistem operasi dan platform yang berbeda, dikenal sebagai teknologi layanan web (Web Services) dan teknologi lain yang mendukung interoperabilitas antarsistem. [10].

Meskipun memiliki berbagai manfaat, cloud computing juga memiliki sejumlah permasalahan yang perlu diperhatikan. Salah satu permasalahan utamanya adalah dalam hal keamanan [6]. Komputasi awan juga membawa risiko tertentu, seperti ketidakjelasan pengguna terhadap lokasi fisik data mereka karena bergantung pada penyedia layanan, kesulitan dalam mengatasi bencana karena ketergantungan pada penyedia layanan untuk pemulihan data, dan potensi masalah jika penyedia layanan mengalami kebangkrutan [9].

ISSN No. 2502-8782



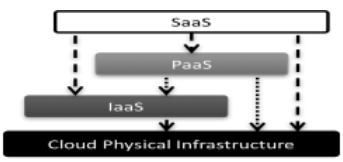
GAMBAR 1. DAMPAK POSOTIF MENGGUNAKAN LAYANAN CLOUD (SUMBER DATABOOKS.GO.ID)

Terlihat pada gambar di atas, 94,1 % respon menjawab bahwa cloud memiliki dampak yang baik dalam kualitas layanan termasuk dalam menyimpan data. Dan dalam tabel 76,5 % beragam layanan meningkat juga ikut termasuk dalam layanan penyimpanan data.

A. LAYANAN CLOUD COMPUTING

Layanan cloud utama disediakan menjadi 3 bagian, diantaranya:

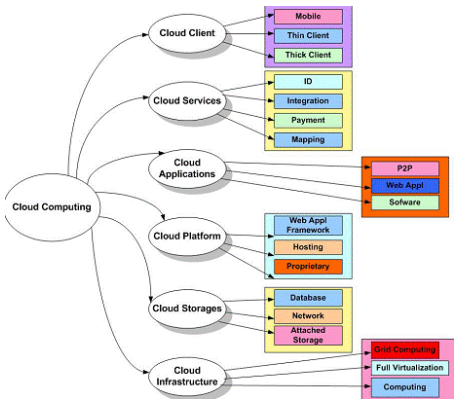
1) IaaS (Infrastructure as a Service), di mana penyedia cloud menyediakan sumber daya komputasi, penyimpanan, dan jaringan sebagai layanan berbasis internet. Model layanan ini didasarkan pada teknologi virtualisasi. Amazon EC2 adalah penyedia IaaS yang paling dikenal [2].
2) PaaS (Platform as a Service), di mana penyedia cloud menyediakan platform, alat, dan layanan bisnis lainnya yang memungkinkan pelanggan untuk mengembangkan, mendeploy, dan mengelola aplikasi mereka sendiri, tanpa menginstal platform atau alat dukungan ini di mesin lokal mereka. Model PaaS dapat dihosting di atas model IaaS atau langsung di atas infrastruktur cloud. Google Apps dan Microsoft Windows Azure adalah PaaS yang paling dikenal [2].
3) Layanan Software as a Service (SaaS) memungkinkan konsumen untuk menjalankan aplikasi menggunakan infrastruktur cloud computing yang telah tersedia. [2].



GAMBAR 2. Cloud Service Delivery Models

Tren terkini mengarah pada penyediaan layanan yang beragam secara terdistribusi dan paralel secara jarak jauh, yang dapat diakses melalui berbagai perangkat. Teknologi ini tercermin dari berbagai metode yang digunakan, mulai dari proses informasi yang dipercayakan kepada pihak luar hingga penggunaan pusat data eksternal (Balboni, 2009). Cloud Computing adalah model yang mendorong konsep layanan yang dikenal sebagai "Semua sebagai Layanan" (XaaS). [1].

GAMBAR 3. Struktur cloud computing



B. KARAKTERISTIK CLOUD COMPUTING DAN IMPLIKASI KEAMANAN

Untuk efisiensi, penyedia cloud perlu optimalkan sumber daya dengan biaya rendah. Penggunaannya harus sesuai kebutuhan, bisa ditingkatkan atau dikurangi sesuai permintaan aktual. Model komputasi awan hadir dengan multitenancy dan elastisitas, menguntungkan kedua belah pihak. Namun, kedua fitur ini berdampak serius pada keamanan cloud. Multitenancy berarti berbagi sumber daya dengan penyewa lain, dengan beberapa cara, seperti pada gambar 2. Pada cara pertama, setiap penyewa punya instansi khusus dengan penyesuaian sendiri. Pada cara kedua, setiap penyewa menggunakan instansi khusus, namun semua instansi tersebut [2].

C. JENIS PENGAMANAN UNTUK CLOUD COMPUTING.

1) User Autentication

Salah satu cara menghindari pencurian akun di cloud computing adalah melalui otentikasi pengguna. Pengguna harus melewati beberapa tahap autentikasi seperti menggunakan username, password, dan single sign-on [4].

a. Username dan password adalah cara yang umum digunakan untuk

mengotentikasi pengguna di cloud computing. Dalam metode ini, pengguna memasukkan kredensialnya yang harus cocok dengan yang disimpan di database penyedia layanan. Namun, username dan password rentan terhadap pembajakan, oleh itu perlu menjaga keamanannya. Beberapa cara meningkatkan keamanan termasuk tidak membagikan kredensial dengan orang lain, menggunakan kombinasi huruf, angka, dan simbol yang kompleks, serta menjaga kerahasiaannya.

b. Single sign-on Selain username dan password, penyedia layanan cloud computing juga dapat menggunakan metode single sign-on. Dengan metode ini, penyedia mempercayakan identitas pengguna kepada pihak ketiga yang disebut penyedia identitas. Sehingga pengguna yang akan menggunakan

aplikasi cloud computing terlebih dahulu diarahkan ke penyedia identitas, jika penyedia identitas dapat memberikan otentikasi, maka pelanggan akan diberikan izin untuk masuk ke aplikasi cloud computing.

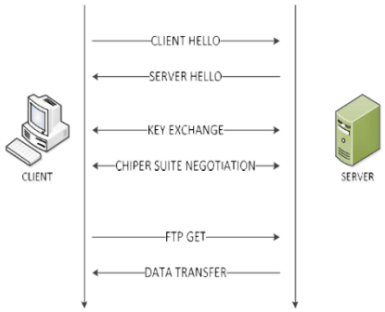
GAMBAR 4. USER AUTENTICATION

2) Enkripsi Data

Selain melindungi keamanan data pengguna, perlu juga meningkatkan keamanan data yang dikirim ke sistem cloud computing. Meskipun aplikasi cloud dilindungi oleh sistem otentikasi dari serangan, perlu diwaspadai bahwa data yang dikirimkan melalui Internet bisa direbut oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting untuk mengenkripsi data yang dikirim agar tidak dapat diakses oleh pihak yang tidak berwenang. Enkripsi data bisa dilakukan baik di sisi pengguna maupun di sisi server. Terdapat beberapa metode enkripsi yang umum, seperti AES, DES, 3DES, dan RSA. [4].

3) SSL (Secure Socket Layer)

Setelah melindungi data dengan enkripsi, langkah berikutnya untuk meningkatkan keamanannya adalah dengan mengamankan jalur komunikasi data. Dalam konteks jaringan komputer, komunikasi data berjalan melalui lapisan TCP/IP. Untuk menjaga keamanannya, penggunaan SSL (Secure Socket Layer) dapat diterapkan untuk mengamankan jalur ini. SSL beroperasi dalam 3 fase: pertama, server dan client berinteraksi untuk menetapkan sistem enkripsi yang akan digunakan; kedua, terjadi pertukaran kunci data enkripsi dengan menggunakan kunci publik; terakhir, pesan dikirim dengan menggunakan kunci enkripsi yang telah ditetapkan sebelumnya.



GAMBAR 5. MEKANISME SSL

4) Kontrol Akses di cloud computing

Kontrol akses adalah kunci keamanan data di Cloud Computing, memastikan hanya pengguna yang sah yang dapat mengakses data di cloud. Berbagai metode seperti Intrusion Detection System, firewall, dan manajemen privilege dapat diterapkan pada berbagai lapisan jaringan dan cloud. Firewall dapat difungsikan untuk menyaring konten yang melewati jaringan cloud, disesuaikan dengan kebijakan keamanan yang ditetapkan oleh pengguna [5].

D. LAYANAN PENYEDIA CLOUD REKOMENDASI

Keamanan data dalam basis data adalah krusial dan sangat peenting bagi organisasi mengingat volume besar data yang tersimpan didalam nya [8]. Sistem rekomendasi menjadi esensial karna sebelumnya ada kekurangan dalam sistem basis konten [8].

1) AMAZON WEB SERVICE (AWS)

AWS Menawarkan berbagai layanan seperti AWS Identity and access management (IAM) untuk mengelola akses pengguna. Mereka memiliki layanan enkripsi yang kuat seperti AWS Key Management Service (KMS) untuk mengamankan data Anda saat istirahat maupun perpindahannya. AWS menawarkan alat monitoring dan deteksi ancaman seperti AWS Guard Duty yang memungkinkan deteksi serangan dan aktivitas mencurigakan di lingkungan cloud.

2) MICROSOFT AZURE
Azure memiliki layanan keamanan yang kuat, seperti Azure Active Directory untuk manajemen identitas dan akses pengguna.
Mereka menawarkan layanan enkripsi data yang kuat seperti Azure Key Vault dan fungsi-fungsi keamanan terintegrasi dalam layanan cloud mereka. Azure Security Center menyediakan pemantauan keamanan dan pelaporan, serta membantu dalam menemukan kelemahan yang mungkin dieksploitasi.

3) GOOGLE CLOUD PLATFORM (GCP)
GCP memiliki layanan keamanan seperti Google Cloud IAM yang memungkinkan pengelolaan akses dan identitas. Layanan enkripsi GCP seperti Google Cloud KMS memberikan kontrol atas kunci enkripsi Anda. GCP juga memiliki layanan monitoring keamanan seperti Google Cloud Security Command Center untuk melacak dan menganalisis keamanan lingkungan cloud Anda.

Ketiga penyedia cloud ini menawarkan alat keamanan kuat untuk melindungi data dan sistem di cloud. Mereka memiliki lapisan keamanan solid mulai dari manajemen akses hingga enkripsi data, pemantauan keamanan, dan deteksi ancaman. Namun, pilihlah layanan yang sesuai dengan kebutuhan bisnis Anda dan pastikan implementasinya sesuai dengan persyaratan keamanan perusahaan Anda.

5. SIMPULAN

Pentingnya keamanan dalam sistem cloud computing tak bisa diabaikan karena risiko kebocoran data, akses yang tidak sah, dan potensi serangan siber. Layanan cloud harus memenuhi standar keamanan industri dengan menerapkan enkripsi data dan autentikasi pengguna yang kuat. Selain itu, penyedia layanan cloud juga harus memiliki praktik keamanan yang kokoh dan sistem pemantauan untuk mendeteksi aktivitas yang mencurigakan.

Hasil penelitian menyoroti dampak positif dan negatif migrasi ke lingkungan cloud, mengidentifikasi ancaman keamanan potensial, serta mengevaluasi strategi perlindungan sistem dan data secara global. Meskipun adopsi cloud computing memungkinkan fleksibilitas dan efisiensi, kekhawatiran akan keamanan menjadi fokus utama. Ancaman seperti akses tidak sah dan kebocoran data harus ditangani dengan langkah-langkah pengamanan seperti autentikasi pengguna dan enkripsi data.

Penyedia layanan cloud besar seperti AWS, Azure, dan GCP menyediakan alat keamanan yang kuat, termasuk manajemen akses, enkripsi data, pemantauan keamanan, dan deteksi ancaman. Namun, penting untuk memilih layanan yang sesuai dengan kebutuhan bisnis dan memastikan implementasinya sesuai dengan persyaratan keamanan yang diperlukan.

Makalah ini memberikan pemahaman mendalam tentang kompleksitas keamanan dalam cloud computing, menyoroti pentingnya strategi keamanan yang terfokus serta solusi terbaik untuk melindungi data dan sistem di lingkungan komputasi awan yang terus berkembang.

6. DAFTAR PUSTAKA

[1]. Yuli Fauziah, 2014*, "Tinjauan Keamanan Sistem Pada Teknologi Cloud Computing".*

[2]. Mohamed Almorsy, John Grundy, Ingo Müller, 2016, *"An Analysis of the Cloud Computing Security Problem".*

[3]. Mohammad Fachry, Ari Kusyanti dan Kasyaful Amron, 2018, *"Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing".*

[4]. Ihsan Taofik, Irawan Afrianto, 2023, *"Analisis Keamanan dan Perlindungan Data pada Komputasi awan dalam ruang lingkup pendidikan".*

ISSN No. 2502-8782

[5]. Munirul Ula, 2019, *"Analisis Metode Pengamanan Data Pada Layanan Cloud Computing"*.

[6]. Issac Odun Ayo, Sanjay Misca dan Olasupo Ajayi, 2018, *"Cloud computing security: Issues and developments"*.

[7]. Mulyana, Irawan Afrianto, 2023, *"Tinjauan Literatur: Analisis Keamanan Sistem Pada Komputasi Awan"*.

[8]. Nedrick Chandra, Ferry,2023, *"Cloud Computing ANALISIS ANCAMAN KEAMANAN DATA DALAM CLOUD COMPUTING"*.

[9]. Satriya, Pratama, 2023, *"PEMANFAATAN TEKNOLOGI SISTEM KOMPUTASI AWAN DALAM PERLINDUNGAN DATA PRIBADI DI INDONESIA"*.

[10]. Adi Nugroho, Techn Khabib Mustofa, 2012, *"IMPLEMENTASI KOMPUTASI AWAN MENGGUNAKAN TEKNOLOGI GOOGLE APP ENGINE(GAE)DAN AMAZON WEB SERVICES(AWS)"*.