Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive

Zulkarnaim Masyhur[1], Adhy Rizaldy[1], Patmayanti Kartini[3]
[1,2,3] Jurusan Sistem Informasi, Universitas Islam Negeri Alauddin Makassar, Indonesia
zulkarnaim.masyhur@uin-alauddin.ac.id[1], adhy.rizaldy@uin-alauddin.ac.id [2], kartinipatmayanti@gmail.com[3]

Informasi Artikel

Article historys:

Di Publikasi Jun 30, 2021

Kata Kunci:

Cloud Computing
Keamanan
Privasi
Google Drive

ABSTRACT

In today's era, we can do mobilization activities anytime and anywhere. Especially with the cloud computing system that makes it easy to interact from one computer to another without consuming a lot of money. This allows us to access data and information from computers or accounts that are connected. Google Drive is a data storage and synchronization service provided by Google. Where every user can use cloud computing in the form of file sharing and editing collaboration. The purpose of this paper is to find out how the challenges and solutions for data security and user privacy are on the Google Drive platform.

Koresponden Author:

Zulkarnaim Masyhur,
Jurusan Sistem Informasi,
Universitas Islam Negeri Alauddin Makassar,
Jl. H.M. Yasin Limpo No. 36 Samata, Kab Gowa, Sulawesi Selatan, Indonesia.

1. PENDAHULUAN

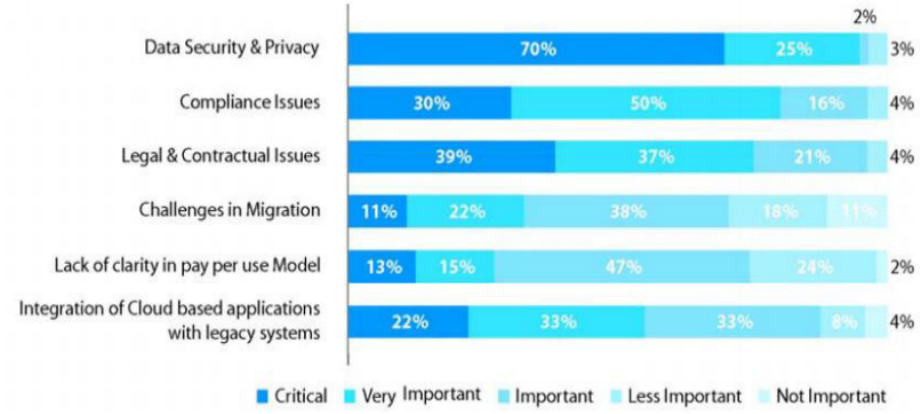
Era teknologi sekarang ini aktifitas dan mobilitas manusia semakin meningkat, teknologi juga berkembang dan mengikuti pola hidup manusia yang membutuhkan kecepatan dan ketersediaan informasi. Data yang merupakan sumber utama informasi saat ini dapat disimpan secara daring sehingga manusia dengan mudah dan kapan saja dapat mengaksesnya. Oleh karena itu banyak sekali masyarakat mencari cara mudah tanpa harus melangkah dari rumah dalam mengakses informasi dan data, di jaman yang sekarang ini banyak kegiatan atau aktivitas masyarakat yang perlu didokumentasikan dan membutuhkan penyimpanan yang cukup besar dan tanpa perlu memikirkan resiko kehilangan data [1]. Perkembangan ilmu pengetahuan dan teknologi saat ini telah mempermudah dan memberi kenyamanan yang berguna dalam mengerjakan tugas sehari-hari yang tidak akan mungkin dapat dikerjakan dalam waktu yang bersamaan. Dalam dunia teknologi informasi dan komunikasi pemanfaatan aplikasi *Cloud computing* adalah salah satu alternative terbaik dalam menyelesaikan masalah diatas. [2]

Cloud computing dapat didefinisikan sebagai gaya komputasi baru di mana sumber daya yang terukur secara dinamis dan sering kali menggunakan konsep virtualisasi yang disediakan oleh provider dengan memanfaatkan media internet. *Cloud computing* telah menjadi trend teknologi yang signifikan, dan banyak ahli berharap bahwa *Cloud computing* akan membentuk kembali proses teknologi informasi (TI) dan pasar TI. [3]

Salah satu aplikasi yang unggul dan umum digunakan adalah Google Drive. Google Drive memberikan layanan penyimpanan gratis sebesar 5 GB dan dapat ditambahkan dengan pembayaran tertentu. Dengan menggunakan fasilitas online dari Google Drive pengguna dapat : *create and collaborate, store everything safely and access it anywhere, search everything, web application connection* [2].

Seperti yang diketahui, *Cloud computing* berkaitan erat dengan privasi dan keamanan data. Kedua hal tersebut sangat penting, mengingat teknologi *cloud* merupakan media penyimpanan

berbasis internet. Jika langkah-langkah keamanan tidak dijaga dengan baik untuk operasi dan transmisi data maka akan berisiko tinggi. Karena *Cloud computing* menyediakan fasilitas bagi sekelompok pengguna untuk mengakses data yang disimpan, ada kemungkinan memiliki risiko data yang tinggi. Langkah-langkah keamanan terkuat harus diterapkan dengan mengidentifikasi tantangan keamanan dan solusi untuk menangani tantangan ini. [4]



Gambar 1. Keamanan dan Privasi Data - Tantangan utama implementasi *Cloud computing*. [4]

Gambar 1 terlihat jelas bahwa keamanan dan privasi data merupakan faktor yang paling penting dan kritis untuk dipertimbangkan. Oleh karena itu, pada makalah ini akan dijelaskan mengenai rincian dan klasifikasi konsep yang terkait dengan *Cloud computing* juga tantangan dan bagaimana solusi keamanan dan privasi data pada sistem *Cloud computing*.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian literature review. Penulis melakukan pencarian referensi terkait dengan keamanan privasi data. Literature review merupakan sebuah metode yang sistematis, eksplisit dan reprodusibel untuk melakukan identifikasi, evaluasi dan sintesis terhadap karya-karya hasil penelitian dan hasil pemikiran yang sudah dihasilkan oleh para peneliti dan praktisi. Beberapa tahapan yang dilakukan dalam peneltian ini yaitu: 1) Menentukan ruang lingkup topik literature yang akan direview, dalam penelitan ini runag lingkup topiknya adalah keamanan dan privasi data sistem *Cloud computing*. 2) Mengidentifikasi sumber rujukan, pada penelitian ini identifikasi dilakukan dengan melihat terbitan dari literatur yang akan direview. 3) Mereview dan menulis review, tahap selanjutnya adalah mengambil subtansi dari setiap referensi yang dikumpulkan kemudian memberikan evaluasi dan menuliskannya kembali.

3. HASIL PENELITIAN DAN PEMBAHASAN

3.1. *Cloud computing*

Cloud computing dapat didefinisikan sebagai lima atribut seperti *Skalabilitas Massive, Multi-tenancy* (berbagi sumber), elastisitas, bayar sesuai penggunaan, dan penyediaan sumber daya sendiri. Elastisitas berarti bahwa sumber daya dapat ditingkatkan ke atas dan ke bawah sesuai kebutuhan [5]. Ini memungkinkan pengguna untuk mengakses file atau data mereka dari komputer mana pun yang memiliki koneksi internet. *Cloud computing* memberikan komputasi yang lebih efisien dengan memusatkan penyimpanan data, pemrosesan dan bandwidth. Teknologi ini berfokus pada virtualisasi server host atau pengontrol utama komputer. Server ini bertindak sebagai jaringan komunikasi di mana informasi dapat dibagikan. Itu informasi dapat disimpan, diambil, dan dibagikan sebagaimana dan bila diperlukan melalui platform global yang tersebar luas.

Cloud computing memungkinkan pengguna untuk mengakses server jarak jauh yang dihosting di internet untuk menyimpan dan memproses data. Memungkinkan pengguna untuk menggunakan teknologi komputer tanpa instalasi di komputer mereka [6]. Model layanan *cloud* diklasifikasikan menjadi tiga jenis seperti SaaS, PaaS, Iaas dan model penyebaran yang berbeda diklasifikasikan ke dalam Private, Publik, dan Hibrida. Karena ketersediaan *cloud* yang tinggi untuk

semua pengguna, *Cloud computing* memiliki lebih banyak keamanan tantangan. Tantangan ini diklasifikasikan ke dalam dua kategori besar sebagai masalah keamanan yang dihadapi oleh penyedia *cloud* dan masalah keamanan yang dihadapi oleh pelanggan [7].

3.2. Keamanan Data

Perhatian utama *cloud computing* adalah perlindungan informasi karena volume data yang sangat besar disimpan di *cloud* dan pengembangan sistem komunikasi, artinya bahwa data dapat diretas atau dihancurkan dari akses yang tidak sah. *cloud computing* menghadapi berbagai masalah keamanan, beberapa di antaranya adalah layanan gangguan, serangan DoS, otentikasi yang disusupi, dan kejahatan luar orang dalam, ancaman keamanan, kerentanan sistem, masalah *multi-tenancy*, integritas data dan privasi data [8]. Pada *cloud computing*, sangat penting untuk mengembangkan keseimbangan pendistribusian data utama yang mengarah pada pemanfaatan sumber daya yang lebih baik dan minimalisasi kesalahan [9].

3.3. Privasi

Sekarang ini penggunaan internet semakin meningkat dan banyak meminta data pribadi. Data-data tersebut biasanya digunakan untuk mengetahui seberapa banyak pengunjung yang ada dan nantinya akan digunakan sebagai analisis dan kebutuhan lain. Data tersebut juga riskan terjadinya penggunaan hak privasi atas data pribadi [10]. Masalah privasi dapat muncul jika informasi sensitif mengenai organisasi atau individu dimuat di layanan *cloud*. Untuk alasan ini, penyedia layanan *cloud* (CSP) menyediakan perlindungan privasi solusi. Namun demikian, tetap rentan terhadap serangan dari penyerang jahat yang menyalahgunakan informasi tanpa otorisasi yang tepat [11].
Pada umumnya terdapat 3 (tiga) aspek dari privasi yaitu mengenai pribadi seseorang (Privacy of a Person's Persona), privasi tentang data seseorang (*Privacy of Data about a Person*), dan privasi atas komunikasi seseorang (*Privacy of a Person's Communication*) [10].

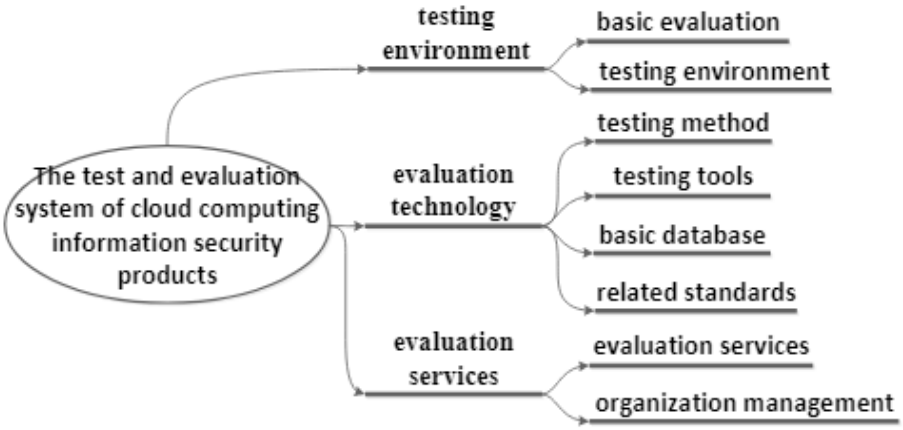
3.4. Google Drive

Google menggabungkan satu set alat kantor lengkap dengan penyimpanan *cloud* di Drive. *User* dapat melakukan pengolahan data dengan layanan ini, termasuk pengolah kata, aplikasi spreadsheet, dan membuat presentasi, kapasitasnya hingga 15 GB ruang penyimpanan gratis. Jika sudah memiliki akun Google, sudah dapat mengakses Google Drive. *User* hanya perlu pergi ke drive.google.com dan mengaktifkan layanan. User mendapatkan 15 GB penyimpanan untuk apa pun yang akan diunggah ke drive, termasuk foto, video, dokumen, file Photoshop, dan banyak lagi. Namun, *User* harus membagikan 15 GB itu dengan akun Gmail, foto yang diunggah ke Google+, dan dokumen apa pun yang dibuat di Google Drive [1].

Dalam menggunakan google drive memerlukan sedikit persiapan jika *user* sudah memiliki akun google. Jika menggunakan Gmail, sangat mudah untuk menyimpan lampiran dari e-mail langsung ke Drive hanya dengan beberapa klik. Aplikasi ini dapat membackup foto sendiri secara otomatis, tanpa perlu aplikasi google foto yang terpisah. Hal ini dapat dilakukan ketika menggunakan google drive untuk membuat dokumen, spreadsheet, atau presentasi, *user* harus mengekspor file-file tersebut untuk mengeditnya di program lain. *User* juga harus berbagi ruang penyimpanan dengan Gmail, jadi jika inbox email sangat banyak maka akan mendapatkan lebih sedikit ruang penyimpanan cloud. Paling baik digunakan untuk pekerja dikantor, atau siapa saja yang menginginkan fasilitas office dengan penyimpanan cloud [1]. Dalam menjaga keamanan data, Google Drive menggunakan metode AES 256. Metode AES adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 256 bit [12].

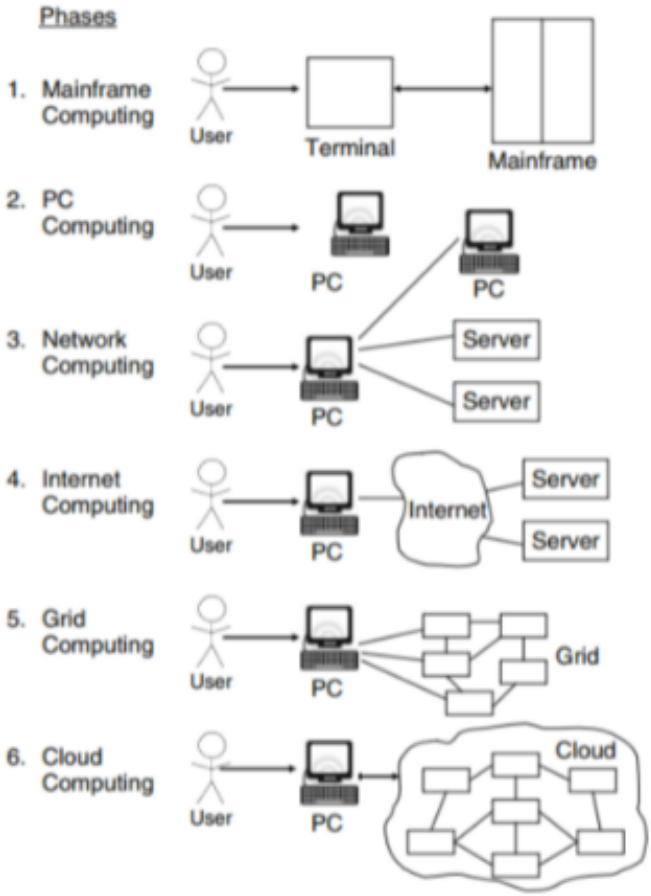
3.5. Konsep *Cloud Computing*

Dalam *cloud computing*, generasi baru teknologi *cloud computing* berkaitan dengan sistem informasi sebagai objek, kebutuhan fungsi keamanan, kebutuhan keamanan itu sendiri dan persyaratan kinerja produk keamanan informasi *cloud computing* diteliti terlebih dahulu, metode dan teknik analisis, dikombinasikan dengan ancaman sistem informasi deteksi kerentanan dan teknologi penilaian risiko, tes *cloud computing* dan sistem evaluasi keamanan informasi produk yang dibuat [13].



Gambar 3. Arsitektur keamanan *Cloud computing* [13]

Konsep *cloud computing* dimulai dengan konsep mainframe computing, user dapat mengakses mainframe melalui sebuah terminal. Dilanjutkan ke fase kedua yaitu PC computing, user dapat mengakses sebuah informasi langsung dari PC. Berkembang fase ketiga yaitu network computing, user dapat mengakses sebuah informasi dari server atau pun perangkat PC yang lain dari sebuah jaringan komputer, user juga dapat mengirimkan sebuah data melalui jaringan komputer. Fase keempat berkembang konsep internet computing, user dapat mengakses informasi dari sebuah PC ke server melalui server. Dengan berkembangnya internet maka pada fase kelima berkembang konsep grid computing dan pada fase keenam yaitu munculnya konsep *cloud computing*, user dapat mengakses sebuah informasi melalui layanan *cloud* [3].



Gambar 4. Konsep *Cloud computing* [3]

3.6. Klasifikasi *Cloud computing*

Cloud computing dapat dikelompokkan menjadi tiga kategori menurut jenis delivery service sebagai berikut:

1. Software as a Service (SaaS) merupakan arsitektur *cloud computing* dimana jenis service ini berupa sejumlah aplikasi-aplikasi yang ditawarkan ke pihak pengguna. SaaS dapat diakses dari jarak jauh oleh pengguna melalui internet berdasarkan model harga yang ditawarkan. Layanan ini akan dikirimkan kepada para pengguna dengan menggunakan aplikasi penyedia yang berjalan dalam infrastruktur *cloud*. Aplikasi dapat diakses dari berbagai perangkat pengguna melalui user interface seperti web browser. Seluruh infrastruktur *cloud* dikendalikan oleh pihak penyedia layanan termasuk jaringan, server, sistem operasi, dan media penyimpanan. Model ini dapat memberikan beberapa manfaat yang sangat menguntungkan baik bagi pengguna maupun penyedia jasa *Cloud computing* [14].
2. Platform as a Service (PaaS) merupakan platform sebagai layanan yang membantu pengguna untuk menyewa berbagai platform, ini cukup menguntungkan untuk waktu yang cepat penyebaran aplikasi sederhana dan hemat biaya juga tidak perlu membeli lapisan perangkat keras dan perangkat lunak [15].
3. Infrastructure as a Service (IaaS) adalah layanan *Cloud computing* yang menyediakan infrastruktur dan perangkat keras seperti server, media penyimpanan, bandwith, virtualisasi, dan konfigurasi lain yang menungkinkan utilitas bagi pengguna. Keuntungan dari layanan IaaS adalah pengguna tidak perlu membeli komputer fisik, sehingga lebih menghemat biaya, konfigurasi komputer virtual juga bisa diubah sesuai kebutuhan [16].

3.7. Tantangan Keamanan

Tugas utama yang tidak kalah penting bagi penyedia layanan *cloud* adalah memastikan bahwa layanan yang tersedia untuk kesiapan data tersedia dengan baik dan dapat diakses dengan mudah oleh pengguna. Seperti adanya masalah keamanan data di *cloud* (*multi-tenancy, loss of control, dan trust*) menjadi fokus utama bagi penyedia layanan *cloud* untuk memastikan bahwa masalah tersebut dapat dikendalikan dan memberikan solusi terbaik jika terjadi masalah. [17]

Untuk menghindari risiko diperlukan pengamanan penyimpanan data dan juga data yang melibatkan penyimpanan, transit, atau proses. Untuk meningkatkan keamanan dalam *Cloud computing*, penting untuk menyediakan otentikasi, otorisasi, dan kontrol akses untuk data yang disimpan di *cloud* [4]. Tiga bidang utama dalam keamanan data adalah :

1. *Confidentiality* : Kerentanan teratas harus diperiksa untuk memastikan bahwa data dilindungi dari serangan apa pun. Jadi uji keamanan harus dilakukan untuk melindungi data dari pengguna jahat seperti Cross-site Scripting, mekanisme Access Control dll.,.
2. Integrity : Untuk memberikan keamanan pada data klien, digunakan hanya sedikit sumber daya yang tersedia. Pengguna tidak boleh menyimpan data pribadi mereka seperti kata sandi agar integritasnya dapat terjamin.
3. *Availability* : Ketersediaan adalah masalah terpenting di beberapa organisasi yang menghadapi downtime sebagai masalah utama. Itu tergantung pada kesepakatan antara vendor dan klien [4].

3.8. AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunkan untuk mengamakan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekripsi data [18]. Adapun putaran kunci algritma AES dapat dilihat pada table 1 berikut:

AES (Bits)	Panjang Kunci (Nk Words)	Ukuran Blok (Nb Words)	Jumlah Putaran (Nr)
AES - 128	4	4	10
AES - 192	6	4	12

AES - 256	8	4	14

Tabel 1. Putaran Kunci Algoritma AES

Algoritma AES menghasilkan pasangan kunci public atau pribadi yang kuat, sebanyak 4096 bit untuk setiap pengguna. Kunci pribadi dienkripsi dengan kata sandi login pengguna menggunakan AES-256. Lalu file membuat kunci ASCII encoded base64 32 byte untuk setiap file, lalu enkripsi file dengan File-key menggunakan AES-256. Dekripsi kunci file dengan private-key dan share-key yang cocok, lalu dekrip file menggunakan kunci file AES-256, yang memiliki panjang kunci 256 bit, mendukung ukuran bit terbesar dan secara praktis tidak dapat dipecahkan oleh *brute force*/serangan brutal berdasarkan daya komputasi saat ini, menjadikannya standar enkripsi terkuat [19].

3.9. Tantangan dan Solusi Keamanan

Cloud computing menimbulkan berbagai masalah keamanan dan privasi, yaitu sebagai berikut:

1. Pengalihdayaan: Pengguna dapat kehilangan kendali atas data mereka. Mekanisme yang tepat diperlukan untuk mencegah penyedia *cloud* menggunakan data pelanggan dengan cara yang belum disepakati di masa lalu.
2. Ekstensibilitas dan Tanggung Jawab Bersama: Ada trade-off antara ekstensibilitas dan tanggung jawab keamanan untuk pelanggan dalam model pengiriman yang berbeda.
3. Virtualisasi: Perlu ada mekanisme untuk memastikan isolasi yang kuat, berbagi yang dimediasi dan komunikasi antara mesin virtual. Hal ini dapat dilakukan dengan menggunakan sistem kontrol akses yang fleksibel untuk menerapkan kebijakan akses yang mengatur kemampuan kontrol dan berbagi VM dalam host *cloud*.
4. Multi-tenancy: Masalah seperti kebijakan akses, penerapan aplikasi, serta akses dan perlindungan data harus diperhitungkan untuk memberikan lingkungan multi-tenant yang aman.
5. Perjanjian Tingkat Layanan: Tujuan utamanya adalah membangun lapisan baru untuk menciptakan mekanisme negosiasi kontrak antara penyedia dan konsumen layanan serta pemantauan pemenuhannya saat dijalankan.
6. Heterogenitas: Penyedia *cloud* yang berbeda mungkin memiliki pendekatan yang berbeda untuk menyediakan mekanisme keamanan dan privasi, sehingga menimbulkan tantangan integrasi. [20]

Confidentiality, Integrity, dan Availability adalah tiga sifat penting dari keamanan data *Cloud computing* dan secara populer disebut sebagai CIA. [21] Google Drive menggunakan model PaaS dalam penerapan *Cloud computing*. Tantangan keamanan PaaS dapat sebagai berikut:

1. Lokasi data : Platform sebenarnya tidak dalam satu host, platform dapat dianggap sebagai kelompok host cluster, sebenarnya lokasi data Anda tidak dapat diisolasi ke sektor tertentu pada host tertentu, ini akan menambah lebih banyak keamanan di atas kepala sejauh satu lokasi lebih mudah untuk mengamankan daripada banyak. Masalah keamanan lainnya adalah bahwa duplikasi dari data menciptakan ketersediaan data yang tinggi untuk pengembang dan pengguna data terdistribusi ini tetap seperti yang lain data perbedaan besar dalam hal ini secara tepat lokasi tidak diketahui.
2. Akses istimewa : Salah satu fitur paling populer di PaaS adalah pengembang perangkat lunak yang diiklankan untuk menggunakan debug. Debug memberikan akses ke data dan lokasi memori untuk memungkinkan pengembang mengubah nilai untuk menguji berbagai hasil, kami menganggap debug menyediakan alat yang diinginkan untuk pengembang dan hacker.
3. Sistem terdistribusi : Sistem file PaaS sangat terdistribusi. Node dapat secara mandiri saat layanan *cloud* provider (CSP) memiliki cluster sehingga kemungkinan besar untuk jalur konfigurasi standar akan tersedia. CSP harus dapat menyediakan yang diperlukan keamanan, tetapi tanggung jawab untuk memverifikasi ini milik klien.

Solusi dan teknik praktis untuk mengatasi serangan ini atau mengurangi dampaknya terdaftar sebagai berikut:

1. Enkapsulasi Akses: Kebijakan kontrol dengan objek dapat menjadi salah satu dari solusi untuk mengatasi akses istimewa
2. Poin Penegakan Kebijakan (PEP): Titik Penegakan Kebijakan (PEP) adalah entitas logis atau tempat di server yang membuat kontrol dan kebijakan penerimaan keputusan dalam menanggapi permintaan dari pengguna yang ingin mengakses sumber daya di komputer atau server jaringan. Dan ini pertimbangkan solusi untuk sistem terdistribusi.
3. Trusted Computing Base (TCB) adalah kumpulan kode yang dapat dieksekusi dan file konfigurasi yang diasumsikan aman. TCB dianalisis secara menyeluruh untuk kelemahan keamanan dan dipasang sebagai lapisan di atas sistem operasi dan menyediakan pemrograman aplikasi standar interface (API) untuk objek pengguna, enkripsi tampaknya menjadi yang terbaik solusi. [22]

Enkripsi disarankan sebagai solusi yang lebih baik untuk mengamankan informasi. Sebelum menyimpan data di server *Cloud computing* lebih baik untuk mengenkripsi data. Pemilik data dapat memberikan izin kepada anggota grup tertentu sehingga data dapat dengan mudah diakses oleh mereka. Keamanan sentris data heterogen akan digunakan untuk menyediakan kontrol akses data. Model keamanan data terdiri dari otentikasi, enkripsi data dan integritas data, pemulihan data, perlindungan pengguna harus dirancang untuk meningkatkan keamanan data melalui *cloud*. Untuk memastikan privasi dan keamanan data, perlindungan data dapat digunakan sebagai layanan. [4]

Penulisan rumus/persamaan/equation ditulis dengan menggunakan fitur equation pada MS Word. Tidak disarankan menggunakan gambar dalam penulisan equation karena kualitas gambar akan berkurang jika di pdf-kan. Penulisan persamaan/equation dapat dilihat pada contoh berikut:

4. KESIMPULAN

Penelitian ini memberikan gambaran tentang berbagai tantangan dan solusi dalam *Cloud computing* dengan menghormati keamanan dan privasi sensitif pengguna data di lingkungan *cloud*. Berdasarkan hasil dari penelitian ini, keamanan data pengguna di *Cloud computing* dapat diketahui bahwa data yang tersimpan di *Cloud computing* tidak bisa diambil dengan mudah begitu saja oleh hacker, user lain atau pun admin dari *cloud* storage, karena data yang tersimpan di *cloud* storage sudah ter-enkripsi Advanced Encryption Standard (AES) yang berbasis 256 keys dimana tidak dapat diakses karena file tersebut sudah terenkripsi.

DAFTAR PUSTAKA

[1] I. Agus, F. Destiawati, and H. Dhika, “Perbandingan Cloud Computing Microsoft Onedrive, Dropbox, dan Google drive,” Fakt. Exacta, vol. 12, no. 1, pp. 20–27, 2019.

[2] A. Nugroho and P. Desa, “Pelatihan pemanfaatan google drive untuk manajemen dokumen dan file di pemerintahan desa sidowangi kabupaten magelang,” no. November, 2019.

[3] “Cloud Computing: Teori dan Implementasi - Yo Ceng Giap, Riki Riki, Didi Kurnaedi, Eko Nursanty, M. Agung Nugroho, Janner Simarmata, Yunita Ardilla - Google Books.” (accessed Jun. 16, 2021).

[4] R. Velumadhava Rao and K. Selvamani, “Data security challenges and its solutions in cloud computing,” Procedia Comput. Sci., vol. 48, no. C, pp. 204–209, 2015, doi: 10.1016/j.procs.2015.04.171.

[5] S. Parikli, D. Dave, R. Patel, and N. Doshi, “Security and privacy issues in cloud, fog and edge computing,” Procedia Comput. Sci., vol. 160, pp. 734–739, 2019, doi: 10.1016/j.procs.2019.11.018.

[6] A. Srinivasan, Q. M. Abdul, and V. Vijayakumar, “Era of cloud computing: A new insight to hybrid cloud,” Procedia Comput. Sci., vol. 50, pp. 42–51, 2015, doi: 10.1016/j.procs.2015.04.059.

[7] G. Manogaran, C. Thota, and M. V. Kumar, “MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing,” Procedia Comput. Sci., vol. 87, pp. 128–133, 2016, doi: 10.1016/j.procs.2016.05.138.

[8] F. Thabit, S. Alhomdy, and S. Jagtap, “A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions,” Int. J. Intell. Networks, vol. 2, no. March, pp. 18–33, 2021, doi: 10.1016/j.ijin.2021.03.001.

[9] D. A. Shafiq, N. Z. Jhanjhi, and A. Abdullah, "Load balancing techniques in cloud computing environment: A review," J. King Saud Univ. - Comput. Inf. Sci., no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.02.007.
[10] "Kriptografi untuk Keamanan Data - Harun Mukhtar - Google Books." (accessed Jun. 17, 2021).
[11] A. Cuzzocrea, C. K. Leung, B. H. Wodi, S. Sourav, and E. Fadda, "An effective and efficient technique for supporting privacy-preserving keyword-based search over encrypted data in clouds," Procedia Comput. Sci., vol. 177, no. 2018, pp. 509–515, 2020, doi: 10.1016/j.procs.2020.10.070.
[12] M. Pandia, "Meningkatkan Keamanan Data Keuangan Dengan Metode Aes Di," pp. 35–40, 2017.
[13] H. H. Song, "ScienceDirect Testing and Evaluation System for Cloud Computing Information Security Products," Procedia Comput. Sci., vol. 166, pp. 84–87, 2020, doi: 10.1016/j.procs.2020.02.023.
[14] A. Almaarif, S. Kom, S. S. Informasi, F. R. Industri, and U. Telkom, "Analysis of Network Performance Cloud With the Quality of Services Method in Microsoft Azure and Amazon Web Services Cloud Computing Technology Provider," vol. 7, no. 2, pp. 6965–6974, 2020.
[15] M. Marliana, "J u r n a l P R O D U K T I F | 331 KEAMANAN DAN PENCEGAHAN DATABASE CLOUD COMPUTING UNTUK PENGGUNA LAYANAN Abstraksi Cloud Computing," vol. 3, no. 2, pp. 331–336, 2019.
[16] "CLOUD COMPUTING: Manajemen dan Perencanaan Kapasitas - Riko Herwanto, Onno W. Purbo, RZ. Abd. Aziz - Google Books." (accessed Jun. 18, 2021).
[17] Maniah, E. Abdurachman, F. L. Gaol, and B. Soewito, "Survey on threats and risks in the cloud computing environment," Procedia Comput. Sci., vol. 161, pp. 1325–1332, 2019, doi: 10.1016/j.procs.2019.11.248.
[18] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," vol. 4, pp. 78–86, 2020, doi: 10.30865/komik.v4i1.2590.
[19] S. T. Ruriawan, "PENGAMANAN DATA CLOUD STORAGE DENGAN MENGGUNAKAN ADVANCED ENCRYPTION STANDARD DAN ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM PADA SECURE SOCKET LAYER BERBASIS WEBSITE SECURING CLOUD STORAGE DATA USING ADVANCED ENCRYPTION STANDARD AND ELLIPTIC CURVE DIGITA," vol. 8, no. 2, pp. 1949–1960, 2021.
[20] F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," Procedia Comput. Sci., vol. 37, pp. 357–362, 2014, doi: 10.1016/j.procs.2014.08.053.
[21] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," Procedia Comput. Sci., vol. 125, no. 2009, pp. 691–697, 2018, doi: 10.1016/j.procs.2017.12.089.
[22] N. H. Hussein and A. Khalid, "A survey of cloud computing security challenges and solutions," Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 1, pp. 52–56, 2016, [Online].