KEAMANAN DAN PENCEGAHAN DATABASE CLOUD COMPUTING UNTUK PENGGUNA LAYANAN

Mella Marliana

STMIK LIKMI, Bandung
e-mail: memarliana@gmail.com

Abstraksi

Untuk mendukung jumlah maksimum pengguna dan layanan yang efektiv dengan sumber daya minimum, penyedia layanan Internet menciptakan komputasi awan. dalam beberapa tahun, komputasi awan yang muncul telah menjadi teknologi yang hangat. Penyampaian Layanan oleh Penyedia Layanan cloud dalam hal DBase penting karena lingkungan cloud memberikan akses ke perangkat keras, perangkat lunak, dan informasi lain yang terpusat. Penyedia layanan database bertanggung jawab untuk menginstal dan memelihara database, dan pemilik aplikasi dikenai biaya sesuai dengan penggunaan layanan. Lingkungan komputasi awan menyediakan platform untuk berbagi sumber daya komputasi dan menyediakan layanan yang berbeda seperti SaaS, PaaS dan IaaS yang akan digunakan oleh organisasi sebagai pribadi, publik atau Hybrid. Komputasi awan pada dasarnya dikenal dengan everything as-a-service. Di komputer pribadi, memiliki kendali penuh atas data dan proses tetapi dalam lingkungan cloudmenggunakan data dan layanan aplikasi yang disediakan oleh beberapa Penyedia Layanan Cloud lainnya. keamanan adalah perhatian utama untuk database dan penyedia cloud membutuhkan kerahasiaan untuk menyimpan data di database. Makalah ini menunjukkan perhatian pada keamanan dan pencegahan Database sebagai Layanan di cloud dengan mencari dari beberapa jurnal yang terpilih yang sudah ada sebagai pengetahuan bagi user yang ingin data base nya di kelola oleh pihak ketiga. Hasil studiliteratur dari berbagai jurnal terkemuka, didapatkan beberapa rekomendasi dalam bentuk tabel yang dikelompokan dalam CIA(Confidenciality, Integrity dan Availability), untuk mengamankan cloud baik untuk user dan penyedia layanan.

Kata kunci: *database, database as a service, security database, mitigation*

Abstract

To support the maximum number of users and effective services with minimum resources, Internet service providers create cloud computing. Within a few years, emerging cloud computing has become a hot topic. Service Delivery by Cloud Service Providers in terms of DBase is important because the cloud environment provides centralized access to hardware, software, and other information. The database service provider is responsible for installing and maintaining the database, and application owners are charged according to the use of the service. The cloud computing environment provides a platform to share computing resources and provides different services such as SaaS, PaaS, and IaaS to be used by organizations as private, public, or Hybrid. Basically, cloud computing is known as everything-as-a-service. On personal computers, have full control over data and processes but in a cloud environment using data and application services provided by several other Cloud Service Providers. Security is a major concern for databases and cloud providers require confidentiality to store data in databases. This paper demonstrates the concern on security and mitigation of Database as a Service in the cloud by searching from selected journals that already exist as knowledge for users who want their database to be managed by third parties. The results of literature studies from various leading journals, obtained several recommendations in the form of tables grouped in the CIA (Confidentiality, Integrity, and Availability), to secure the cloud for both users and service providers.

Keywords*: database, database as a service, database security, prevention*

PENDAHULUAN

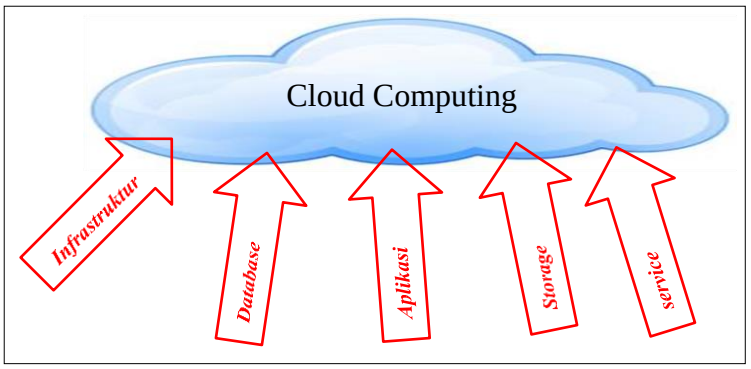
Salah satu tantangan utama bagi perusahaan TI saat ini adalah bagaimana mengelola volume data yang semakin besar dan untuk menghasilkan produk perangkat lunak yang berkualitas untuk memastikan pemanfaatan sumber daya yang optimal dengan biaya minimum. Untuk mendukung jumlah maksimum pengguna dan layanan yang efektif dengan sumber daya minimum, penyedia layanan Internet menciptakan *Cloud Computing*. dalam beberapa tahun, *Cloud Computing* yang muncul telah menjadi teknologi yang hangat. Penyampaian layanan oleh penyedia layanan *cloud* dalam hal DBase penting karena lingkungan *cloud* memberikan akses ke perangkat keras, perangkat lunak, dan informasi lain yang terpusat. Dengan database sebagai model layanan, pemilik aplikasi tidak perlu menginstal dan memelihara database itu sendiri. Sebaliknya, penyedia layanan database bertanggung jawab untuk menginstal dan memelihara database, dan pemilik aplikasi dikenai biaya sesuai dengan penggunaan layanan mereka.

Sistem manajemen basis data c*loud* adalah basis data terdistribusi yang memberikan komputasi sebagai layanan, bukan produk. Ini adalah berbagi sumber daya, perangkat lunak, dan informasi antara beberapa perangkat melalui jaringan yang sebagian besar merupakan internet. Lingkungan c*loud computing* menyediakan platform

 ISSN: 2548-8082/ E-ISSN 2615-6350
Vol 4 No. 2 Edisi 2020

untuk berbagi sumber daya komputasi dan menyediakan layanan yang berbeda seperti SaaS, PaaS dan IaaS yang akan digunakan oleh organisasi sebagai pribadi, publik atau Hybrid. Komputasi awan pada dasarnya dikenal dengan *Everything as-a-service*.
Karena komputasi awan digunakan bersama sumber daya terdistribusi di seluruh dunia jaringan luas (misalnya internet)
di lingkungan terbuka, sehingga akan menimbulkan berbagai masalah keamanan di lingkungan *cloud* dan aplikasinya. Di komputer pribadi, memiliki kendali penuh atas data dan proses tetapi dalam lingkungan *cloud* menggunakan data dan layanan aplikasi yang disediakan oleh beberapa penyedia layanan cloud lainnya. keamanan adalah perhatian utama untuk database dan penyedia *cloud* membutuhkan kerahasiaan untuk menyimpan data di database. Dalam tulisan ini menunjukkan perhatian pada keamanan dan *pencegahan* database sebagai layanan di *cloud* dengan mencari dari beberapa jurnal yang terpilih yang sudah ada sebagai pengetahuan bagi user yang ingin data base nya di kelola oleh pihak ketiga.

Cloud Computing adalah model untuk memungkinkan akses jaringan di mana-mana, nyaman, sesuai permintaan ke kumpulan bersama sumber daya komputasi yang dapat dikonfigurasi (misalnya, jaringan, server, penyimpanan, aplikasi, dan layanan) yang dapat disediakan dan dirilis dengan cepat dengan upaya manajemen minimal atau interaksi penyedia layanan. [1]. Ada lima layanan dalam *cloud computing* lihat Gambar 1



Gambar 1 Lima Macam Layanan Cloud [2]

1. Layanan *Cloud Computing*
   Ada lima layanan dalam *cloud computing* yaitu[2][3][4][5][6]:
   a. Perangkat lunak sebagai layanan (***Sas***), membantu pengguna untuk memanfaatkan perangkat lunak dan juga menghilangkan kebutuhan untuk menginstal dan menjalankan perangkat lunak pada sistem mereka sendiri. Berbagai vendor menyediakan perangkat lunak yang disewa dengan menggunakan middleware, operating sistem, virtualisasi, server, penyimpanan, dan jaringan. „Aplikasi Google‟ adalah salah satu contoh layanan **Saas**.
   b. Platform sebagai layanan (***Paas***), 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. Pada dasarnya, browser internet akan digunakan untuk mengembangkan aplikasi (Google chrome, Mozilla Firefox). „Force.com ' adalah contoh layanan **Paas**.
   c. Infrastruktur sebagai layanan (***Iaas***), untuk meminimalkan biaya pembelian infrastruktur. Sebaiknya mengambil informasi jaringan dengan basis sewa. Pengguna memanfaatkan sebagai infrastruktur di atas yang dapat mereka instal apa saja platform yang dibutuhkan. *Amazon ec2*, ruang rak, *windows azure*, *Google compute* engine adalah contoh layanan **Iaas**.
   d. Penyimpanan sebagai layanan (**Staas**), menyediakan fasilitas untuk pengambilan pengguna server yang disewakan. Untuk membeli server secara fisik adalah tugas yang cukup mahal, ada baiknya untuk menyewa server dan membayar hanya untuk waktu tertentu kita menggunakannya. *'Amazon s3'* adalah contoh dari **Staas**.
   e. Database sebagai layanan (***Dbaas***), membantu pengguna untuk menyediakan database sesuai permintaan pengguna sehingga dapat diakses melalui internet dari penyedia layanan database *cloud*. *'Oracle exadata'* adalah contoh layanan **Dbaas** [7].

2. Karakteristik *Cloud Computing*[1][8][9]
   a. Layanan mandiri sesuai permintaan. Seorang konsumen dapat secara sepihak menyediakan kemampuan komputasi, seperti waktu server dan penyimpanan jaringan, sesuai kebutuhan secara otomatis tanpa memerlukan interaksi manusia dengan setiap penyedia layanan.
   b. Akses jaringan yang luas. Kemampuan tersedia melalui jaringan dan diakses melalui mekanisme standar yang mempromosikan penggunaan oleh platform klien yang heterogen (misalnya, ponsel, tablet, laptop, dan workstation).
   c. Pengumpulan sumber daya. Sumber daya komputasi penyedia dikumpulkan untuk melayani banyak konsumen menggunakan model *multi-tenant*, dengan sumber daya fisik dan virtual yang berbeda

ditetapkan secara dinamis dan ditetapkan ulang sesuai dengan permintaan konsumen. Ada rasa kemandirian lokasi di mana pelanggan umumnya tidak memiliki kendali atau pengetahuan atas lokasi yang tepat dari sumber daya yang disediakan tetapi mungkin dapat menentukan lokasi di tingkat abstraksi yang lebih tinggi (misalnya, negara, negara bagian, atau pusat data). Contoh sumber daya termasuk penyimpanan, pemrosesan, memori, dan bandwidth jaringan.

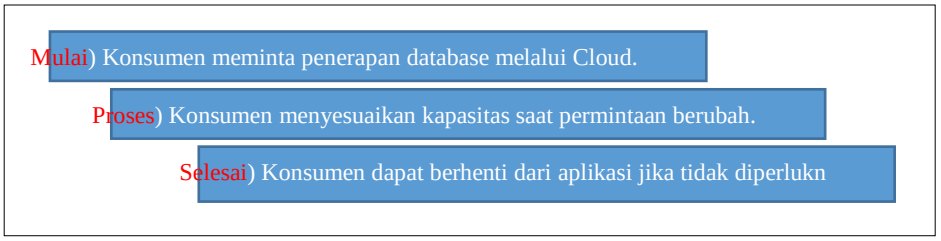
d. Elastisitas yang cepat. Kapabilitas dapat disediakan dan dilepaskan secara elastis, dalam beberapa kasus secara otomatis, untuk menyesuaikan dengan cepat ke luar dan ke dalam yang sesuai dengan permintaan.

Bagi konsumen, kemampuan yang tersedia untuk penyediaan seringkali tampak tidak terbatas dan dapat disesuaikan dalam jumlah berapa pun dan kapan pun.

e. Layanan terukur. Sistem *cloud* secara otomatis mengontrol dan mengoptimalkan penggunaan sumber daya dengan memanfaatkan kapabilitas pengukuran pada beberapa tingkat abstraksi yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, bandwidth, dan akun pengguna aktif). Penggunaan sumber daya dapat dipantau, dikendalikan, dan dilaporkan, memberikan transparansi bagi penyedia dan konsumen layanan yang digunakan.

3. Layana *Cloud* Database

Layanan database menyediakan secara otomatis konsumen bisa meminta fungsionalitas dari layanan khusus yang dihosting di *Cloud*. Ada banyak layanan basis data lain yang tersedia saat ini tetapi layanan database berbeda dari basis data tradisional karena arsitekturnya memiliki dua atribut utama yaitu: Berorientasi layanan karena fasilitas basis data tersedia dalam bentuk layanan. Model interaksi layanan mandiri pelanggan karena organisasi diizinkan untuk menggunakan, mengonfigurasi, dan menyebarkan layanan database *Cloud* itu sendiri tanpa dukungan TI apa pun dan tanpa membeli perangkat keras apa pun untuk tujuan yang ditentukan. Tiga fase utama dalam arsitektur layanan database secara keseluruhan lihat gambar 2.



Gambar 2. Tiga Fase Utama Arsitektur Layanan Databse Cloud [9]

4. Struktur Empat Lapis Keamanan Layanan Database[9][10]

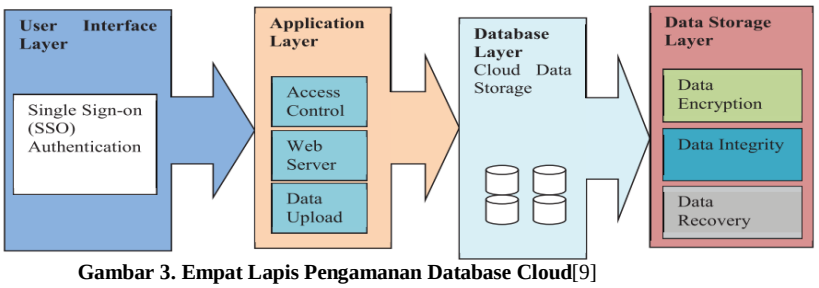
Model yang ditunjukkan pada gambar 3. menggunakan struktur sistem empat lapis, setiap lapis melakukan tugasnya sendiri untuk memastikan keamanan data dari lapisan *Cloud*.

a. Lapisan pertama: bertanggung jawab untuk otentikasi pengguna, menggunakan otentikasi kata sandi satu kali. *User Interface Layer* digunakan untuk mengakses layanan melalui internet. Hal ini memungkinkan pengguna dengan mudah memanfaatkan layanan database yang dapat diskalakan dan elastis yang tersedia di infrastruktur *Cloud*.

b. Lapisan kedua: digunakan untuk mengakses layanan perangkat lunak dan ruang penyimpanan di *Cloud*. Seperti yang dinyatakan sebelumnya, konsumen tidak perlu memiliki sumber daya perangkat keras untuk memanfaatkan layanan ini.pelanggan hanya upload data pengguna dan melakuan kontrol akses.

c. Lapisan ketiga menyediakan layanan yang efisien dan handal untuk mengelola database yang berada di *Cloud* dan memungkinkan penggunaan kembali kueri yang berada di penyimpanan, sehingga menghemat waktu untuk membuat kueri dan memuat data.

d. Lapisan keempat adalah lapisan penyimpanan data, di mana Data dienkripsi dan didekripsi pada masing-masing tahap penyimpanan dan pengambilan. Integritas data dan pemulihan data juga disediakan di lapisan ini.



Gambar 3. Empat Lapis Pengamanan Database Cloud[9]

5. Prinsip Keamanan Informasi [11][12][11]

Keamanan sistem informasi bertujuan untuk menjaga integritas, ketersediaan, dan kerahasiaan sumber daya sistem informasi (termasuk perangkat keras , perangkat lunak, informasi / data, dan telekomunikasi). Konsep keamanan kerahasiaan, integritas dan ketersediaan juga disebut triad CIA [13].

a. Kerahasiaan informasi biasanya dilihat sebagai jaminan bahwa informasi sensitif hanya diakses oleh pengguna yang berwenang. Tugas ini dapat dicapai dengan berbagai mekanisme seperti enkripsi dan kontrol akses.
b. Integritas informasi biasanya dilihat sebagai jaminan bahwa informasi tidak di rubah oleh pengguna yang tidak sah sedemikian rupa sehingga pengguna yang sah yang akan dapat merubahnya. Tugas ini dapat dicapai dengan berbagai mekanisme seperti tanda tangan digital dan kode otentikasi pesan.
c. Ketersediaan adalah tugas untuk memastikan bahwa suatu sistem menyediakan layanannya kepada penggunanya kapan saja. Biasanya sebuah sistem mencakup banyak mekanisme untuk memastikan ketersediaannya, seperti penggunaan beberapa sumber daya independen dan beberapa jalur komunikasi.

METODE PENELITIAN

Hasil dari studi literatur dengan mengumpulkan bebrbagai jurnal yang terkemuka dan dengan kunci pencarian layanan database cloud. Dari sekian banyak pencarian dianalisis yang berhubungan dengan keamanan data base sebagai layanan di cloud. Dari beberapa jurnal yang relevan dipilih dan dikelompokan menjadi bagian dari *confidenciality, integrity* dan *availability*

HASIL DAN PEMBAHASAN

Layanan database cloud harus memperhatikan berbagai ancaman dan pencegahan dilihat dari aspek keamanan (CIA) secara menyeluruh, dapat dilihat pada tabel 1.

Tabel 1. Ancaman dan Pencegahan Berdasarkan CIA

No.	Ancaman	Pencegahan	CIA
1	Ancaman Orang Dalam	◦ Karyawan dapat memanfaatkan data sensitif dan rahasia . ◦ Manajemen dan penilaian rantai pasokan yang ketat diperlukan	*Confidenciality*
2	Penyerang dari luar Berbahaya	◦ Serangan berbahaya oleh peretas. ◦ Tidak adanya otentikasi, otorisasi dan akuntansi kontrol dapat mengakibatkan serangan	*Confidenciality*
3	Masalah Kontrol Akses	◦ Pemilik data tidak dapat menentukan atau mengubah kebijakan sesuai kebutuhan. ◦ Peningkatan biaya pengembangan dan analisis terjadi saat pengelolaan pengguna dan akses *granular* kontrol diterapkan	*Confidenciality*
4	Pemulihan Data Ilegal dari Perangkat Penyimpanan	◦ Lakukan *degaussing*, pemusnahan dan penimpaan data untuk menghindari kebocoran data. ◦ Pemulihan data oleh sumber berbahaya jika tidak dibuang dengan benar	*Confidenciality*
5	Pelanggaran Jaringan	◦ Data yang mengalir melalui jaringan (internet) rentan terhadap keadaan berbahaya dan masalah kinerja jaringan. ◦ Kemungkinan penyebab kegagalan jaringan adalah: kesalahan konfigurasi, kurangnya isolasi sumber daya, kelangsungan bisnis yang buruk atau belum teruji, rencana pemulihan bencana, modifikasi lalu lintas jaringan	*Confidenciality*
6	Asal Data	◦ Kompleksitas dan kepekaan waktu dalam metadata asal. ◦ Perhitungan intensif terlibat dalam mendapatkan riwayat yang dibutuhkan. ◦ Algoritma cepat, log otomatis diperlukan	*Confidenciality*
7	Kegagalan Rantai Pasokan	◦ Keamanan bergantung pada pihak ketiga saat data dialihdayakan	*Confidenciality*
8	Lokalitas Data	◦ Masalah kepatuhan dan keamanan data, undang-undang privasi melarang perpindahan data sensitif antar negara. ◦ Masalah yang dihadapi ketika tidak ada yang bertanggung jawab atas data di lokasi penyimpanan data *independen*	*Confidenciality*
9	Yurisdiksi yang Bervariasi	◦ Resiko dan batasan yang dihadapi ketika data pelanggan tunduk pada yurisdiksi hukum beberapa negara. ◦ Data dalam situasi ini dapat diakses oleh banyak pihak	*Confidenciality*
10	*Arsitektur Proxy*	◦ Mengurangi kebutuhan penggunaan komponen perantara. Metadata dipindahkan ke database. Mesin enkripsi dijalankan oleh setiap klien. ◦ Skalabilitas, keamanan dan konsistensi data	*Confidentiality*
11	Homo-morphic penuh	◦ kueri terenkripsi data algoritma dimungkinkan. ◦ Evaluasi Algoritma digunakan selain pembuatan kunci, enkripsi dan dekripsi	*Confidentiality*

12	Alogaritma pribadi	· Enkripsi tidak digunakan. Nilai atribut dibagi ke beberapa server terdistribusi berdasarkan mekanisme berbagi rahasia. · Penyedia layanan tidak dapat menyimpulkan konten data. · Perpanjangan metode ini hanya mengambil yang diperlukan, bukan keseluruhan database.	*Confidentiality*
13	Solusi Penyimpanan Data *Cryptonite-Secure*	· Menangani persyaratan ketersediaan. Pemilik file memiliki izin untuk mengenkripsi dan mengaudit data.	*Confidentiality*
		· Memungkinkan manajemen kunci yang terukur dan mengamankan file.	
14	Model NetDB2 multi-share	· Mendukung arsitektur NetDB2. · Berdasarkan algoritma berbagi rahasia. · Komunikasi jaringan yang aman. · Data dibagi menjadi bagian 'n'	*Confidentiality*
15	Berbagi algoritma rahasia	· Data dibagi menjadi bagian "n" dan didistribusikan ke beberapa server. · Seluruh database diambil untuk rekonstruksi data, melibatkan overhead pemrosesan.	*Confidentiality*
16	Jaminan eksekusi	· Pemilik data memastikan eksekusi kueri yang aman berdasarkan mekanisme hashing.	*Confidentiality*
17	Enkripsi homomorfik	· Beroperasi pada ukuran blok yang lebih besar. · Perhitungan berlaku langsung pada ciphertext. · Server database tidak dapat melihat / mengakses kunci / data	*Confidentiality*
18	Arsitektur Net DB2	· Berdasarkan kriptografi (baik RSA dan Blowfish). · TLS dan SSL digunakan untuk privasi. · Informasi tidak diungkapkan ke layanan penyedia	*Confidentiality*
19	Manajemen harus konsisten	· Saling ketergantungan antara server replika berkurang. · Ada jalur maksimum yang dapat diandalkan antara server primer ke semua server replika	*Integrity*
20	Mekanisme Audit Integritas Penyimpanan	· Kode data penghapusan terdistribusi digunakan untuk menggunakan redundansi. · Token homomorfik digunakan untuk menyimpan data secara dinamis. · Mengaudit log	*Integrity*
21	Menjaga Privasi Audit Publik untuk Penyimpanan Cloud yang Aman	· Auditor pihak ketiga digunakan untuk komunikasi dengan pengguna untuk memeriksa integritas data. · Audit batch digunakan untuk melakukan tugas audit yang didelegasikan dari pengguna yang berbeda. · Menggunakan Enkripsi homomorfik berbasis kunci publik pengautentikasi linier.	*Integrity*
22	Integritas verifikasi kueri	· Pengguna / kueri, dapat memverifikasi kueri yang dieksekusi dan dukungan untuk pertanyaan *JOIN* dan *AGGREGATE*	*Integrity*
23	Penyimpanan data	· Enkripsi sisi klien dengan cepat digunakan. · Menggunakan Algoritma SHA-512 untuk kontrol integritas. · AES-256 digunakan untuk enkripsi. · Pengguna tidak lagi harus mengelola kunci secara manual.	*Integrity*
24	Pemeriksaan Integritas	· Modifikasi konfigurasi, akses dan file data merupakan ancaman terhadap integritas data. · Membutuhkan akurasi dan integritas data	*Integrity*
25	*Resource Exhaustion*	· Pemodelan yang tidak sesuai dengan kebutuhan pelanggan menyebabkan *Resource Exhaustion*	*Availability*
26	Internet mati	· Masalah jaringan (internet) memengaruhi kinerja	*Availability*
27	*Data Lock-In*	· Pelanggan tidak dapat memindahkan data dari satu situs ke situs lainnya. · Kegagalan layanan yang disediakan oleh satu vendor akan mengakibatkan hilangnya data secara keseluruhan. · Perlu API standar untuk dijalankan di bawah platform setiap penyedia	*Availability*
28	Bencana Alam	· Kurangnya rencana pemulihan bencana. · Aplikasi yang tidak diuji secara memadai dapat menjadi ancaman bagi ketersediaan layanan.	*Availability*
29	Kurangnya Audit dan Pemantauan	· Audit diperlukan untuk menghindari kegagalan, pemeliharaan cadangan, · Konfigurasi mekanisme kegagalan otomatis untuk memastikan keamanan data. · Persyaratan konfigurasi berubah terus menerus. · Membutuhkan jaringan dan perangkat fisik, keahlian sumber daya manusia	*Availability*

30	Pendekatan Pencadangan	، Server cadangan disimpan di lokasi yang jauh. ، Meode enkripsi dan dekripsi tradisional digunakan dengan dua langkah autentikasi. ، Enkripsi dilakukan selama operasi pencadangan.	*Availability*

KESIMPULAN

Kesimpulan dari penelitian ini didapatkan beberapa keamanan layanan database *cloud* yang sudah di kelompokan menjadi CIA(*Confidentiality*, *Integrity* dan *Availability*), dengan layanan tersebut akan meminimalkan beberapa infrastruktur dan sumber daya manusia dengan harga yang relatif murah. Karena beberapa kelebihan layanan database cloud yang ditawarkan oleh penyedia layanan, sehingga memberikan pengetahuan baik pelanggan yang berniat ingin memindahkan database ke *Cloud* harus memperhatikan keamanan. Saran dari hasil penelitian ini bisa dilakukan dengan melakukan pencarian journal dengan batasan waktu yang lama, sehingga mendapatkan pilihan jurnal yang lebih banyak untuk mengelompokan menjadi *Confidentiality, Integrity dan Availability*.

DAFTAR PUSTAKA

[1] G. A. Osorio, C. S. Del Real, C. A. F. Valdez, M. C. Miranda, and A. H. Garay, "The NIST Definition of Cloud Computing," *Spec. Publ. 800-145*, vol. 728, pp. 269–274, 2006.
[2] A. Sharma and S. Sharma, "STORAGE OF DATABASE ON CLOUD WITH SECURITY," no. 9, pp. 74–77, 2015.
[3] M. Alam and K. A. Shakil, "Cloud Database Management System Architecture Object-Oriented Database," no. July, pp. 978–981, 2013, doi:10.3850/978-981-07-5461-7.
[4] Y. E. Gelogo and S. Lee, "Database Management System as a Cloud Service," *Int. J. Futur. Gener. Commun. Netw.*, vol. 5, no. 2, pp. 71–76,2012.
[5] H. J. Bhatti and B. B. Rad, "Databases in Cloud Computing: A Literature Review," *Int. J. Inf. Technol. Comput. Sci.*, vol. 9, no. 4, pp. 9–17,2017, doi: 10.5815/ijitcs.2017.04.02.
[6] C. Omputing, "F RAMEWORK F OR S ECURE C LOUD," *Int. J. Cloud Comput. Serv. Archit.*, vol. 3, no. 2, pp. 21–35, 2013.
[7] D. Bijwe, "Database in Cloud Computing-Database-as-a Service (DBaas) with its Challenges," *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 2, pp. 73–79, 2015, [Online]. Available: www.ijcsmc.com.
[8] D. Winn, "Getting Started with Cloud Foundry," *Cloud Comput.*, vol. 5931, no. June, pp. 224–231, 2009, doi: 10.1007/978-3-642-10665-1.
[9] K. Munir, "Security model for cloud database as a service (DBaaS)," *Proc. 2015 Int. Conf. Cloud Comput. Technol. Appl. CloudTech 2015*,2015, doi: 10.1109/CloudTech.2015.7336974.
[10] A. Izang, O. Okoro, and O. Taiwo, "Computer Science Security and Ethical Issues To Cloud," no. December, 2017.
[11] S. Aldossary and W. Allen, "Data Security , Privacy , Availability and Integrity in Cloud Computing : Issues and Current Solutions," vol. 7, no.4, 2016.
[12] H. Hacigümüş, B. Iyer, and S. Mehrotra, "Ensuring the integrity of encrypted databases in the database-as-a-service model," *IFIP Adv. Inf.Commun. Technol.*, vol. 142, pp. 61–74, 2004, doi: 10.1007/1-4020-8070-0_5.
[13] A. Shabtai, Y. Elovici, and L. Rokach, "Data Leakage Detection/Prevention Solutions," *SpringerBriefs Comput. Sci.*, no. 9781461420521, pp.17–37, 2012, doi: 10.1007/978-1-4614-2053-8_4.

Biodata Penulis

Mella Marliana. Memperoleh gelar Sarjana Pendidikan (S.Pd.) di Universitas Pendidikan Indonesia (UPI) lulus tahun 2003. Saat ini sedang melanjutkan pendidikan Pasca Sarjana Magister Sistem Informasi Bisnis di STMIK LIKMI Bandung. *E-mail saya* *memarliana@gmail.com*