OPEN ACCESS
J. OF ICT, VOL. 4, NO. 1, PP.085-091, JUNE 2022

ISSN : 26861089 (ONLINE)
DOI: 10.52661

Journal of Informatics and Communications Technology (JICT)

Analisis Keamanan dan Kenyamanan pada Cloud Computing

Dwina Satrinia [#1], Syifa Nurgaida Yutia [#2], Iik Muhamad Malik Matin [#3]

#1,2 *Teknologi Informasi, Institut Teknologi Telkom Jakarta*
Jalan Daan Mogot KM.11, Jakarta 11710 Indonesia

[1] dwina@ittelkom-jkt.ac.id
[2] syifanurgaida@ittelkom-jkt.ac.id

#3 *Teknik Informatika dan Komputer, Politeknik Negeri Jakarta*
Jalan Prof. DR. G.A. Siwabessy, Kampus Universitas Indonesia, Depok 16425 Indonesia

[3] iik.muhamad.malik.matin@tik.pnj.ac.id

Received on dd-mm-yyyy, revised on dd-mm-yyyy, accepted on dd-mm-yyyy

Abstract

Cloud computing atau 'komputasi awan' menyajikan berbagai kemudahan untuk organisasi maupun individu dalam mengakses data dimanapun dan kapanpun. *Cloud computing* memiliki kelebihan seperti memberikan berbagai pilihan model layanan, jenis penyimpanan data, serta pengaturan komputasi yang sesuai kebutuhan sehingga memberikan manfaat yang menarik yaitu efisiens, efektif dan hemat biaya. Kelebihan tersebut tidak membuat *cloud computing* aman dari ancaman serangan keamanan. Konsep keamanan dibutuhkan untuk membantu manajemen pada organisasi maupun individu dalam melindungi dan melakukan pengamanan data pada layanan cloud. Selain itu, model kenyamanan juga diperlukan untuk membantu pengguna dalam menggunakan layanan cloud.

Keywords: *cloud computing*, komputasi awan,

I. PENDAHULUAN

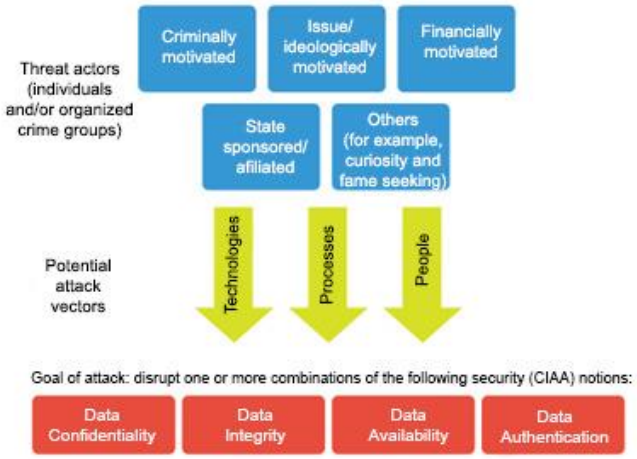
Cloud computing berkaitan dengan layanan teknologi informasi yang melibatkan jaringan internet secara efisien sehingga memudahkan organisasi atau individu dalam memanfaatkan sumber daya virtual. Suatu organisasi atau individu yang menggunakan layanan *cloud computing* dari pihak ke-3 yaitu *cloud provider* harus memahami bahwa pengolahan data pribadi terdapat pada sistem yang dikelola oleh pihak ketiga. Selain itu *cloud computing* menggunakan konsep "*multi tenancy*", dimana beberapa pelanggan lain mungkin menjalankan proses pada hardware fisik yang sama sehingga pelanggan harus percaya bahwa komputasi mereka aman dari pihak lain yang tidak sah. Pelanggan juga harus memahami bagaimana fitur keamanan yang ditawarkan oleh cloud provider untuk melindungi komputasi mereka [3].

Beberapa keuntungan yang didapat dari perspektif pengguna *cloud computing* adalah kapasitas sesuai permintaan, biaya kepemilikan yang rendah, dan harga yang fleksibel, menimbulkan minat yang kuat untuk investasi dari industri maupun pemerintah dan juga meningkat pada organisasi dan individu, sedangkan dari

perspektif *cloud provider*, keuntungan mencakup konsolidasi sumber daya, manajemen yang seragam, dan biaya operasional yang efektif [4]

Namun, selain keuntungan yang ditawarkan, juga menyebabkan potensi masalah keamanan dan privasi. Masalah keamanan dan privasi disebabkan dari penggunaan yang ilegal dan informasi yang tidak etis, yang menyebabkan pengungkapan informasi rahasia, hal tersebut dapat secara signifikan dapat menghalangi pengguna mengimplementasi layanan berbasis *cloud* [4].

Cloud computing telah menjadi target serangan yang potensial, bukan hanya kehilangan data yang merupakan masalah tetapi juga ketersediaan, maka diperlukan melihat setiap peristiwa yang mungkin terjadi dan tentukan dampaknya [9]. Pelaku serangan bisa dari individu ataupun dari organisasi yang tergabung dalam grup dengan motif kejahatannya bisa karena kriminal, Isu / ideology atau karena finansial, mereka menyerang dari berbagai macam aspek serangan dengan target utama yaitu melumpuhkan pertahanan "C, I, A, A" yaitu *confidentiality*, *integrity*, *availability* dan *authentication* yang dijabarkan pada gambar 2 [9]:



Gambar 1 Threat actors and potential attack vectors [9]

Pada Gambar 1 ancaman aktor penyerang dapat mengeksploitasi satu atau lebih banyak aspek serangan yang potensial, contohnya yaitu *embedding malware*, dimana seseorang dapat mengganggu satu atau lebih kombinasi dari *confidentiality*, *integrity*, *availability* dan *authentication* [9] melalui rekayasa sosial dan *process* seperti kebijakan dan prosedur.

Untuk menanggulangi ancaman tersebut diperlukan penerapan keamanan *cloud computing* yang memadai sehingga sistem *cloud computing* dapat memberikan perlindungan keamanan terhadap data bisnis atau data organisasi yang berharga walaupun data dan sistem disimpan dan dijalankan di *cloud* serta dikelola oleh penyedia layanan. Berdasarkan latarbelakang tersebut, maka paper ini berisi tentang bagaimana penerapan keamanan *cloud computing* yang bisa diterapkan oleh organisasi maupun individu untuk menanggulangi ancaman serangan keamanan data *confidentiality*, *integrity*, *availability*, *authentication* dan bagaimana model kenyamanan pada *cloud computing*.

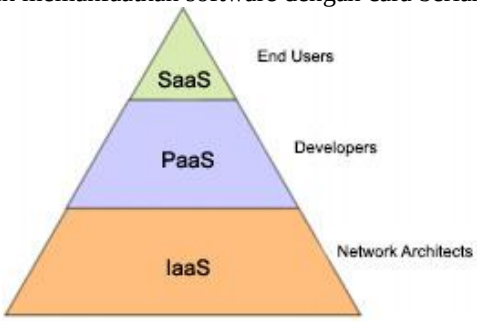
II. LANDASAN TEORI

A. Pengertian Cloud Computing

Pengertian dari cloud computing menurut National Institute of Standards and Technology (NIST) yaitu suatu model yang memungkinkan pembagian sumber daya komputasi sehingga dapat dipakai bersama secara mudah serta dapat dikonfigurasi sesuai kebutuhan dan sesuai permintaan [1]. Definisi lain dari *cloud computing* adalah suatu kumpulan komputer yang saling terhubung sehingga menjadi suatu sistem terdistribusi dan paralel, yang tervirtualisasi secara dinamis ditetapkan dan disajikan berdasarkan perjanjian serta negosiasi antara cloud provider dan pelanggan sebagai satu atau lebih sumber daya komputasi serta layanan terpadu [2].

Jenis Layanan *cloud computing* pada pengguna mengacu pada persyaratan dan tujuan *cloud computing* yang akan digunakan. Terdapat tiga jenis model layanan cloud yang biasanya disediakan cloud provider yaitu

Infrastructure as a Service (IaaS) yang biasa digunakan oleh system admin atau arsitek jaringan untuk memenuhi kebutuhan infrastrukturnya, Platform as a Service (PaaS) yang biasa digunakan oleh developer untuk mengembangkan aplikasi ke lingkungan cloud, dan Software as a Service (SaaS) yang biasa digunakan oleh end user atau pengguna awam untuk memanfaatkan software dengan cara berlangganan [7], [8]:



Gambar 2 Model Layanan Cloud Computing [8]

Software As a Service (SaaS): Menyediakan layanan sumber daya perangkat lunak / software yang dihosting di suatu server cloud kepada konsumen sesuai dengan kebutuhan mereka. *Platform As a Service* (PaaS): Dimana cloud provider menyediakan infrastruktur serta akses platform, yang memungkinkan mereka untuk menempatkan perangkat lunak mereka sendiri yang disesuaikan dan aplikasi lain di *cloud*. Sedangkan *Infrastruktur As a Service* (IaaS): memungkinkan pelanggan menyewa sumber daya server untuk pemrosesan komputasi, penyimpanan, serta konektivitas jaringan [7], [8].

B. Karakteristik Cloud Computing

Setidaknya terdapat lima karakteristik yang harus dipenuhi layanan *cloud computing* menurut National Institute of Standard and Technology (NIST) Amerika Serikat, yaitu [1]:

- *On demand self service*
  Pengguna atau pelanggan dapat memesan dan mengelola layanan secara mandiri, tanpa interaksi dengan *cloud provider*, misalnya pemesanan dilakukan melalui sebuah portal web yang terdapat antarmuka untuk kemudahan pemesanan dan pengelolaan layanan. Layanan akan terjadi secara otomatis pada penyedia yang dapat digunakan oleh pelanggan.
- *Broad network access*
  Akses jaringan yang luas dimana kemampuan suatu jaringan dapat diakses melalui mekanisme standar serta dapat digunakan pada berbagai platform (misalnya, smartphone, laptop, dan PDA).
- *Resource pooling*
  Penyedia layanan atau cloud provider menyatukan sumber daya komputasi yang dimilikinya seperti storage, memori, pemrosesan, *bandwidth* jaringan, dan mesin virtual agar dapat melayani beberapa pelanggan dengan layanan sementara dan skalabel sesuai kebutuhan dari setiap pelanggan. Umumnya para pelanggan tidak mengetahui lokasi dari server yang disewanya, namun masih dapat menentukan lokasi di tingkat wilayah yang lebih tinggi seperti negara atau negara bagian, zona atau region dari data centernya.
- *Rapid elasticity*
  Layanan cloud computing yang dapat ditetapkan ketersediaannya dan skalabilitas yang fleksibel dan cepat sesuai dengan kebutuhan.
- *Measured Service*
  Penggunaan sumber daya dari sistem cloud dapat diawasi, dikendalikan, dioptimalkan dan dilaporkan pengunaannya secara otomatis dengan memanfaatkan kemampuan pengukuran (metering) contohnya pengukuran pada penyimpanan, *bandwidth*, pemrosesan, dan *account* pengguna aktif yang sesuai dengan jenis layanan yang digunakan. Pengukuran tersebut memberikan kenyamanan bagi pelanggan dalam hal transparansi dari layanan yang digunakan oleh pelanggan yang diberikan oleh penyedia layanan.

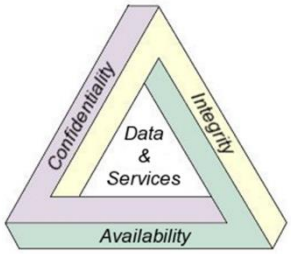
C. Cloud Deployment Model

Model penerapan cloud computing (Cloud deployment model) terbagi menjadi 4 yaitu *Private Cloud*, *Community Cloud*, *Public Cloud* dan *Hybrid Cloud* [1]*:*

- *Private Cloud*
  Private cloud merupakan layanan cloud dimana infrastrukturnya dibangun secara khusus untuk memenuhi kebutuhan internal suatu perusahaan. *Private cloud* ini biasanya dibangun oleh departemen IT pada suatu perusahaan, dan mereka yang memiliki, mengoperasikan, mengatur dan menyediakan layanan untuk departemen lain di perusahaan yang sama.
- *Public Cloud*
  Berbeda dengan private cloud dimana layanan hanya tersedia untuk perusahaan yang sama, public cloud menyediakan layanan *cloud computing* untuk umum dapat bersifat gratis ataupun berbayar. Pengguna dapat menggunakan layanan dengan mengikuti ketentuan yang berlaku dari cloud provider.
- *Community Cloud*
  Cloud computing yang digunakan atau dibangun secara eksklusif untuk komunitas tertentu yang memiliki konsentrasi pada bidang yang sama.
- *Hybrid Cloud*
  Hybrid cloud menggabungkan dua atau lebih jenis *cloud development* (*private, public, atau community*) dimana perusahaan dapat memilih atau memisahkan proses bisnis mana yang dapat diakses secara public cloud, dan proses bisnis mana saja yang diterapkan sebagai *private cloud*.

D. Konsep Keamanan Informasi

Dr M.E. Whitman dan H.J Mattord menyatakan bahwa terdapat aspek penting dalam keamanan informasi. Dalam buku mereka yang berjudul "*Principles of Information Security",* menyebutkan bahwa Confidentiality, Integrity dan Availability atau disebut juga C.I.A *triangle* merupakan hal yang perlu diperhatikan dalam keamanan informasi. [11]



Gambar 3 CIA Triangle

Gambar 3 merupakan gambar CIA Triangle dimana *Confidentiality* artinya sistem harus bisa menjamin bahwa yang dapat mengakses informasi hanya yang memiliki hak saja sehingga dapat mencegah bocornya informasi kepada pihak yang tidak bertanggung jawab. *Integrity* berhubungan dengan kelengkapan informasi yang terjamin serta terjaga dari kerusakan atau ancaman lain yang dapat menyebabkan perubahan informasi dari aslinya. Sedangkan asplek *Availability* adalah aspek yang menjamin pengguna dapat mengakses informasi dalam format yang dapat digunakan tanpa adanya gangguan [11].

Terdapat juga tambahan keamanan informasi selain CIA *triangle* yaitu *privacy*, *identification*, *authentication*, *authorization* dan *accountability*[11]. Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi untuk tujuan tertentu dan hanya dapat digunakan khusus bagi pemilik data harus terjaga keamanannya dari orang lain. Hal tersebut merupakan tujuan dari aspek *Privacy*. Aspek keamanan *Identification* merupakan aspek keamanan dimana system dapat mengenali individu penggunanya. Aspek Identifikasi adalah langkah awal yang perlu dilewati untuk memperoleh hak akses ke suatu informasi yang diamankan. Contoh penerapan identifikasi yang umum digunakan adalah penggunaan username atau user ID serta password saat akan mengakses suatu informasi. Aspek *Authentication* merupakan aspek keamanan yang terjadi saat sistem dapat membuktikan bahwa pengguna yang sedang mengklaim identitas merupakan pengguna yang sah, yang memang memiliki identitas tersebut. *Authorization* merupakan proses selanjutnya setelah proses otentikasi terjadi, dimana sistem dapat menjamin bahwa pengguna telah mendapatkan hak yang khusus dan jelas untuk mengakses, mengubah isi informasi atau menghapus informasi. Aspek yang terkahir yaitu *Accountability* dimana aspek ini terpenuhi jika sistem dapat memberikan data aktifitas yang terjadi terhadap aset informasi, dan siapa saja yang melakukan aktifitas tersebut [11].

Maka jika dilihat dari konsep berikut, dalam kasus lingkungan *cloud computing*, *confidentiality* berarti cara mengamankan data penyedia *cloud* serta pelanggan lainnya, *Integrity* berarti data yang tersimpan pada server *cloud* tidak boleh dimodifikasi atau diubah oleh pengguna yang tidak sah, *availability* jika pelanggan mengakses layanan *cloud* maka harus tersedia dengan format yang diminta pengguna karna jika layanan tidak bisa diakses maka pelanggan tidak akan percaya pada sistem *cloud* dan *authentication* serta *authorization* yaitu layanan *cloud* harus dapat membuktikan identitas pengguna serta memastikan pengguna tersebut memang benar-benar pemilik identitas yang sah dan memberikan hak akses sesuai dengan haknya pada aset informasi yang diamankan.

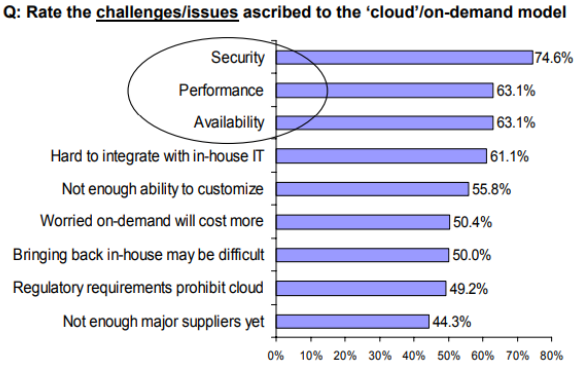
E. Konsep Kenyamanan Cloud Computing

X. Zheng pada penelitiannya mengajukan model pengukuran kualitas layanan *cloud* bernama CLOUDQUAL [15]. CLOUDQUAL memiliki enam dimensi kualitas yaitu *usability, availability, reliability, responsiveness, security, dan elasticity*. Dimensi *usability* bersifat subjektif, sedangkan dimensi lain bersifat objektif. *Usability* menjelaskan seberapa mudah, efisien, dan menyenangkan *interface* ke layanan *cloud* digunakan, atau menilai kemudahan pemanggilan fungsi layanan *cloud* melalui API (*Application Programming Interface*). Bagi *end-user* yang tidak memiliki keahlian di bidang *cloud*, GUI (*Graphical User Interface*) lebih dipilih dibanding API. Lebih lagi, WUI (*Web User Interface*) lebih baik dibanding GUI. Pengguna perlu melakukan instalasi *client* GUI, sedangkan dengan WUI pengguna tidak perlu melakukan *instalasi*.

III. STUDI KASUS & SOLUSI

A. Studi Kasus

Sebuah survey yang dilakukan oleh lembaga IDC pada Gambar 4 menunjukan 74% perusahaan IT memilih keamanan sebagai tantangan teratas yang jadi kekhawatiran dalam penerapan *cloud computing* [5].



Gambar 4 IDC Enterprise Panel August 2008 [5]

Pada hasil survey diatas terlihat bahwa tantangan dalam penerapan *cloud computing* setelah *security* adalah *performance* dan *availability* dengan sama-sama menunjukan nilai persentase yang sama yaitu 63,1%. Sebuah contoh kasus yang pernah terjadi menyerang *availability dan performance* pada *cloud computing* yaitu serangan DOS yang serangan terhadap server berbentuk pengiriman paket data secara terus menerus membuat server semakin melambat, dan dapat mengakibatkan server tumbang jika paket data yang dikirimkan ke server terlalu besar dan banyak. Serangan DOS pernah terjadi pada hari Jumat (21/10/2016) Jam 07.10 UTC dimana serangan tersebut menyerang server Dyn DNS yang menyebabkan sejumlah layanan online besar menjadi lambat bahkan tidak dapat diakses. Server yang terkena serangan tersebut merupakan server yang memiliki banyak pengguna secara global di seluruh dunia dan digunakan oleh perusahaan besar ternama seperti GitHub, Twitter, Spotify, dan lain-lain sehingga serangan ini terbilang cukup fatal [6].

B. Solusi

Dari studi literature yang telah dilakukan dapat dibuat suatu pendekatan penerapan keamanan pada *cloud computing* untuk memberikan solusi melindungi serangan terhadap data *confidentiality*, *integrity*, *availability* dan *authentication.*

1. *Authentication and Identity Management* [12]

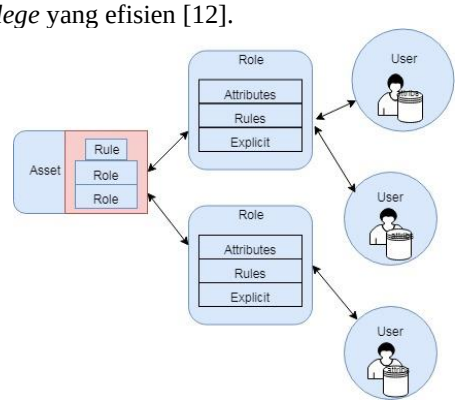
Pengguna dapat mengakses informasi dari berbagai tempat melalui internet sehingga kita memerlukan mekanisme *Authentication* dan *Identity Management* (IDM) untuk mengotentikasi pengguna dan memberikan layanan kepada mereka berdasarkan kredensial dan karakteristik. Jadi Sistem IDM harus dapat melindungi informasi yang bersifat pribadi dan sensitif yang terkait dengan pengguna dan prosesnya. Setiap perusahaan memiliki kebijakan masing – masing dalam sistem manajemen identitasnya untuk mengatur kontrol akses ke sumber daya komputasi dan informasi.

2. *Data Centric Security and Protection* [12]

Dalam *cloud computing*, pengguna dapat berbagi, menyimpan, dan mengakses data melalui *cloud*. Jadi data dari satu pengguna harus dipisahkan dengan baik dari yang lain dan harus aman dari satu lokasi ke lokasi lain [12]. Penyedia *Cloud* dalam hal ini yaitu *cloud provider* harus menerapkan langkah-langkah keamanan yang tepat agar tidak terjadi kebocoran data atau pencurian akses dari pihak yang tidak sah. Kebijakan kontrol akses harus diterapkan dengan benar. Ketika seseorang ingin mengakses data, sistem harus memeriksa aturan kebijakannya dan dapat diterima hanya jika kebijakannya terpenuhi. Pendekatan kriptografi dan aturan kebijakan pengguna harus diperhatikan. Teknik kriptografi yang ada dapat dimanfaatkan untuk keamanan data.

3. *Access Control Needs* [12]

Kebutuhan akses kontrol di antara banyak metode yang diusulkan sejauh ini, berbasis peran yaitu RBAC atau *Role Based Access Control* telah diterima secara luas sebagai model yang paling menjanjikan karena kesederhanaannya, fleksibilitas dalam menangkap persyaratan dinamis, dan dukungan untuk *least privilege* dan manajemen *privilege* yang efisien [12].

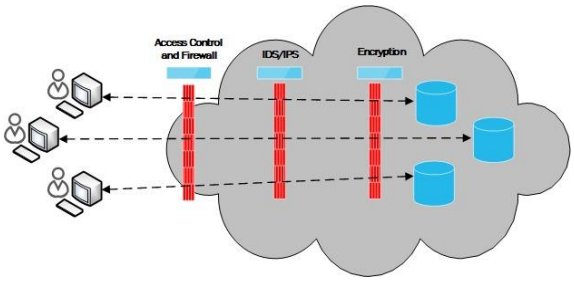


Gambar 5 Role Based Access Control

Kelebihan penerapan *Role Based Access Control* (RBAC) yaitu : pengelolaan izin pengguna skala besar yang efisien, baik dari segi waktu dan usaha, penegakan prinsip kontrol akses yang efektif dan efisien, dapat dicapai oleh penugasan pengguna ke *role* dan dengan penugasan *role permission*, pengauditan izin pengguna yang disederhanakan untuk kepatuhan terhadap peraturan [13].

4. *Firewall* dan IDS/IPS [14]

Pada mekanisme keamanan berlapis yang tertera pada Gambar 6, layer pertama menggunakan *access control* dan *firewall* untuk untuk membatasi akses pada pengguna yang sah. Pada layer kedua terdapat *Intrusion Detection System* atau *Intrusion Prevention System* (IDS/IPS) untuk memaksimalkan perlindungan sistem dari berbagai serangan seperti virus, *worm*, *trojan*, akses tidak sah, dan DoS, kemudian lapis ketiga menggunakan *encryption* untuk pengamanan data [14].



Gambar 6 Cloud Computing Adoption Framework Multi-Layered Security

IV. KESIMPULAN

Pendekatan keamanan yang diusulkan dapat dijadikan solusi serangan keamanan pada *cloud computing* jika diterapkan dengan baik oleh organisasi maupun individu. Ancaman serangan pada data *confidentiality* dapat diatasi dengan penerapan *data centric security and protection* dengan teknik kriptografi untuk pengamanan data pada *cloud computing.* Serangan pada data *integrity* dapat menerapkan *access control* dengan metode *role based access control* sehingga dapat menjamin data tidak diubah oleh pengguna yang tidak berhak dan juga dengan penerapan enkripsi data. Serangan data *accountability* dapat diterapkan *authentication and identity management* dan untuk serangan data *availability* dapat menerapkan *access control, firewall* dan juga IDS/IPS. Untuk kenyamanan pada *cloud computing* dapat menggunakan model pengukuran kualitas layanan *cloud* yaitu CLOUDQUAL yang terdiri dari penerapan *Application Programming Interface* (API), *Graphical User Interface* (GUI) serta *Web User Interface* (WUI) untuk memudahkan penggunaan *cloud computing*.

DAFTAR PUSTAKA

[1] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” National Institute of Standards and Technology Special Publication 800-145, Department of Commerce, Gaithersburg, 2011.

[2] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Bandic, I.: Cloud Computing and emerging IT platforms: vision, hype, and relatity for deliverling computing as the 5th utility. Future Generation Computer System 25(6), 599–616 (2009)

[3] Trent Jaeger and Joshua Schiffman, “Outlook: Cloudy with a Chance of Security Challenges and Improvements,” in IEEE Security and Privacy, 8(1), 77–80. doi:10.1109/MSP.2010.

[4] Z. Tari, "Security and Privacy in Cloud Computing," in IEEE Cloud Computing, vol. 1, no. 1, pp. 54–57, 2014.

[5] Gens, F.: New IDC IT Cloud Services Survey: Top Benefits and Challenges. In: IDC eXchange (2008)

[6] Bonguet, Adrien dan Belaiche, Martine, “A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing” (2017)

[7] Farhan Bashir Shaikh and Sajjad Haider, “Security Threats in Cloud Computing”, 6th International Conference on Internet Technology and Security Transaction, in IEEE Cloud Computing, 2011.

[8] Sarvesh Kumar, Saurabh Srivastava, Vijay Kumar, Ramashare Yadav, Kapil Sharma, “Cloud Computing with Real Life Case Studies and a new approach of solving security issues and putting data in cloud”,International Journal of Computer Science Engineering & Information Technology Research,3,1,149-154,2249-6831,March,2013

[9] Kim-Kwang Raymond Choo, “A Cloud Security Risk Management Strategy”, in IEEE Cloud Computing, 2014.

[10] Bernd Grobauer, Tobias Walloschek, and ElmarStocker, “Understanding Cloud Computing Vulnerabilities”, copublished by the IEEE Computer and Reliability Societies 1540-7993/2011 IEEE March/April 2011

[11] Principles of Information Security, 4th Ed. - Michael E. Whitman (2012)

[12] Takabi, H., Joshi, J.B.D, “Security and privacy challenges in cloud computing environment” in IEEE Journal on Security and Privacy, 1540-7993/10/$26.00, 2010

[13] Virginia N.L. Franqueira, VF InfoSec Consulting Roel J. Wieringa, “Role Based Access Control in Retrospect” in IEEE Journal on Computer Society, June 2012

[14] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138-151, 1 Jan.-Feb. 2016.

[15] X. Zheng, P. Martin, K. Brohman and L. D. Xu, "CLOUDQUAL: A Quality Model for Cloud Services," in IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1527-1536, May 2014.