Analisis Teknik-Teknik Keamanan Pada *Cloud Computing dan* NEBULA (*Future Cloud*): *Survey Paper*

Beny Nugraha

Universitas Mercu Buana

*(Corresponding author) benynugraha@mercubuana.ac.id**

Abstract*— Cloud computing is one of the networking technology that is constantly improving, this is a result of cloud computing's advantages which are able to improve the flexibility and the capability of the computer process without having to spend big investment to build a new infrastructure. Security analysis of the security mechanisms that has been implemented as well as the mechanisms that is still being developed is conducted in this research. Those security mechanisms will be compared based on its ability to handle the security attacks that might occur in cloud computing. In The attack centric method is used in this research, each security attack will be analyzed on how it works, and then which security mechanism that can mitigate that security attack can be identified. There are four security attacks that are analyzed in this research. The result from this research is the NEBULA, the future cloud computing architecture, has the most secure security mechanisms, namely Proof of Consent (PoC), Proof of Path (PoP), and a new cryptography technique called ICING. These three techniques plus the current internet mechanisms such as onion routing are able to mitigate the security attacks that are analyzed in this research.

Keyword; cloud computing, cryptography, nebula, network security, security mechanism

I**ntisari*— ***Cloud computing **adalah salah satu dari teknologi jaringan yang sedang berkembang pesat saat ini, hal ini dikarenakan *cloud computing* memiliki kelebihan dapat meningkatkan fleksibilitas dan kapabilitas dari proses komputer secara dinamis tanpa perlu mengeluarkan dana besar untuk membuat infrastruktur baru, oleh karena itu, peningkatan kualitas keamanan jaringan *cloud computing* sangat diperlukan. Penelitian ini akan meneliti teknik-teknik keamanan yang ada pada *cloud computing* saat ini dan arsitektur *cloud computing* masa depan, yaitu NEBULA. Teknik-teknik keamanan tersebut akan dibandingkan dalam hal kemampuannya dalam menangani serangan-serangan keamanan yang mungkin terjadi pada *cloud computing*. Metode yang digunakan pada penelitian ini adalah metode *attack centric*, yaitu setiap serangan keamanan dianalisis karakteristiknya dan kemudian diteliti mekanisme keamanan untuk menanganinya. Terdapat empat serangan keamanan yang diteliti dalam penelitian ini, dengan mengetahui bagaimana cara kerja sebuah serangan keamanan, maka akan diketahui juga mekanisme keamanan yang mana yang bisa mengatasi serangan tersebut. Dari penelitian ini didapatkan bahwa NEBULA memiliki tingkat keamanan yang paling tinggi. NEBULA memiliki tiga teknik baru yaitu Proof of Consent (PoC), *Proof of Path* (PoP), dan teknik kriptografi ICING. Ketiga teknik tersebut ditambah dengan teknik *onion routing* dapat mengatasi serangan keamanan yang dianalisa pada penelitian ini.**

Kata Kunci; cloud computing, kriptografi, serangan keamanan, mekanisme keamanan, nebula

I. PENDAHULUAN

Cloud computing adalah salah satu dari teknologi jaringan yang sedang berkembang pesat saat ini, hal ini dikarenakan *cloud computing* memiliki kelebihan dapat meningkatkan fleksibilitas dan kapabilitas dari proses komputer secara dinamis tanpa perlu mengeluarkan dana besar untuk membuat infrastruktur baru. Hal ini juga akan memperkecil keluarnya biaya dalam melatih ahli-ahli yang baru maupun dalam hal perizinan perangkat lunak yang baru. Seperti telah didefinisikan oleh USA *National Institute of Standard Technology* (NIST), *cloud computing* dapat memberikan kenyamanan akses bagi para penggunanya, serta dapat secepatnya dirilis dengan interaksi yang minimal dengan para penyedia layanan [1]. NIST juga menyebutkan bahwa *cloud computing* adalah sebuah paradigma yang baru dalam teknologi jaringan karena dapat memberikan fleksibilitas yang tinggi namun dengan biaya yang rendah. *Cloud computing* dapat mencakup berbagai macam aspek kehidupan manusia, seperti contohnya adalah penggunaan situs-situs media sosial dalam kehidupan sehari-hari.

Seiring dengan semakin berkembangnya *cloud computing*, peningkatan performa dalam soal keamanan ketersediaan jaringan menjadi sangat penting. Hal ini dikarenakan *cloud computing* sangat berkaitan dengan pengaksesan aplikasi perangkat lunak dan penyimpanan data secara online, sehingga harus tersedia kapanpun dibutuhkan. Menurut *Cisco Global Cloud Index*, banyaknya data yang tersimpan dalam cloud computing pada akhir 2017 akan mencapai 7.7 zettabytes (7.7 x 1021 bytes) [2]. Oleh karena itu, peningkatan kualitas keamanan serta ketersediaan *jaringan cloud computing* sangat diperlukan.

Masalah pada jaringan saat ini seperti masalah fleksibilitas diharapkan dapat diatasi dengan sedang dikembangkannya sebuah jaringan *cloud computing* masa depan, yang diberi nama NEBULA. Untuk mengetahui tingkat keamanan dari NEBULA, maka penelitian ini akan meneliti dan membandingkan beberapa teknik keamanan yang dapat diaplikasikan pada jaringan *cloud computing* saat ini dan NEBULA.

Ida Bagus et al. [3] telah melakukan penelitian pada jaringan nirkabel yang menghasilkan kesimpulan bahwa perlu penambahan mekanisme keamanan yang menggunakan kombinasi antara server otentikasi, *firewall*, serta WPA/WPA2 untuk dapat menutup celah keamanan dan meningkatkan mekanisme keamanan jaringan nirkabel. Sugiyanto [4] dan Andrew et al. [5] telah membuat sistem dan aplikasi yang menggunakan SMS *gateway*, namun penelitian mereka tidak membahas keamanan sistem tersebut yang memiliki basis yang sama dengan cloud computing saat ini yaitu *address based* (berbasiskan alamat). Rahamatullah et al. [6] telah melakukan survey mekanisme keamanan pada beberapa jaringan internet masa depan, diantaranya adalah NEBULA, namun penelitian tersebut memfokuskan pada mekanisme keamanan antar jaringan internet masa depan dan tidak membandingkan dengan jaringan internet saat ini. Oleh karena itu, pada penelitian ini akan dibandingkan mekanisme keamanan pada jaringan *cloud* saat ini dengan jaringan *cloud* masa depan (NEBULA).

Pada penelitian ini diteliti teknik-teknik yang memang telah digunakan maupun teknik-teknik yang masih dalam proses pengembangan. Dalam penelitian ini akan ditentukan teknik keamanan yang paling tepat untuk diaplikasikan ke dalam arsitektur *cloud computing*, serta membandingkan tingkat keamanan dari jaringan *cloud computing* saat ini dengan jaringan NEBULA.

II. METODOLOGI PENELITIAN

A. Metodologi *Attack Centric*

Metode yang diterapkan untuk melakukan penelitian ini adalah metode *Attack-Centric*. Metode ini dilakukan dengan tiga langkah berikut: Pertama, menganalisa apakah tujuan dari serangan tersebut (contoh: untuk menganalisis jenis trafik dengan menangkap dan menganalisis paket-paket data yang ada pada trafik tersebut). Kedua, menganalisa bagaimana sebuah serangan dapat terjadi (contoh: menentukan titik di mana seorang penyerang harus mengawasi paket-paket yang melintas). Ketiga, menentukan mekanisme keamanan apa yang diperlukan untuk mencegah serangan tersebut. Contoh hasil pada metode ini adalah sebagai berikut: Jika sebuah serangan telah dianalisa adalah serangan yang bertujuan untuk menangkap dan menganalisis paket-paket data, maka mekanisme keamanan yang dibutuhkan untuk mencegah serangan tersebut adalah dengan melakukan mekanisme *anonymous connection* kepada semua user yang ada dalam jaringan. Hal ini akan mencegah seseorang untuk menentukan titik di mana dia harus mengawasi paket dikarenakan IP *Address user* yang ada dalam jaringan akan tersembunyi.

B. Analisis Teknik-Teknik Keamanan Pada *Cloud Computing*

Pada metode ini akan dianalisis beberapa teknik keamanan jaringan yang telah diaplikasikan pada *cloud computing* maupun teknik yang masih dalam proses pengembangan. Analisis akan dilakukan dengan cara meneliti bagaimana cara kerja dari teknik-teknik keamanan tersebut.

Setelah dua metode di atas dilakukan, langkah terakhir adalah menentukan vulnerabilitas kemanan dari *cloud computing* serta kapabilitas dari setiap teknik keamanan yang dianalisis. Kapabilitas dari setiap teknik keamanan akan dibandingkan, sehingga akan dapat diketahui teknik keamanan yang lebih berpotensi untuk diterapkan pada *cloud computing* secara maksimal. Teknik keamanan yang akan diusulkan adalah yang memiliki kapabilitas dalam menangani serangan keamanan yang paling baik, serta lebih efisien dibandingkan dengan teknik yang lainnya. Tingkat ke-efisienan suatu teknik keamanan dapat ditentukan dari tingkat kompleksitas teknik keamanan tersebut.

III. IDENTIFIKASI SERANGAN KEAMANAN

Pada penelitian ini, terdapat 4 serangan keamanan yang akan diteliti, di mana serangan tersebut akan menyebabkan kebocoran data. Serangan-serangan keamanan tersebut adalah:

1) *Snooping Attack*

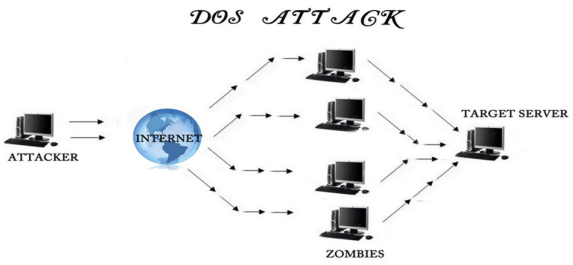
Snooping attack adalah kondisi dimana seorang penyerang akan melihat paket data yang mengalir di dalam jaringan. *Snooping attack* bersifat pasif, penyerang tidak akan memodifikasi paket data yang telah dia lihat [7]. Seorang penyerang akan mengambil konten-konten yang tersimpan pada komputer *user*, sehingga menyebabkan kebocoran data.

2) *Traffic Analysis Attack*

Traffic analysis attack adalah serangan yang dilakukan oleh seorang penyerang dengan cara menganalisis pergerakan trafik untuk mengekstrak informasi dari pola trafik. Dengan serangan ini, seorang penyerang dapat melihat konten-konten apa saja yang diminta oleh *user*, dengan demikian si penyerang dapat mengetahui konten apa saja yang tersedia pada server, apabila konten tersebut berharga baginya, si penyerang dapat memasuki server untuk mengambil konten tersebut.

3) *Denial of Service (DOS) Attack*

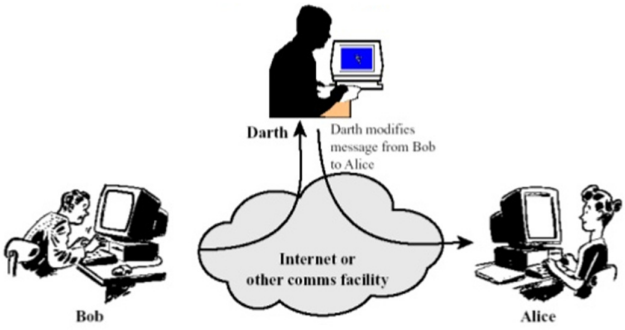
DoS attack adalah serangan yang bertujuan untuk membuat sebuah server atau website tidak dapat diakses oleh *user* lain. Salah satu contoh serangan yang dapat dilakukan adalah dengan membanjiri jaringan dengan paket-paket sampah [8]. Dengan menerapakan serangan ini, server penyedia *cloud* akan menjadi *down*, sehingga dapat dengan mudah dimasuki oleh seorang penyerang. Gambar 1 berikut mengilustrasikan *DoS Attack*.



Gambar 1. Ilustrasi *DoS Attack*

4) *Man-In-The-Middle (MITM) Attack*

Si penyerang akan berada di tengah-tengah *user* dan server *cloud* yang sedang berkomunikasi untuk menginisiasi *man-in-the-middle attack* [9]. Serangan ini adalah salah satu penyebab utama kebocoran data, hal ini dikarenakan si penyerang dapat mengambil data yang mengalir antara *user* dan server penyedia konten dalam *cloud*. *User* dan server tidak dapat mengetahui bahwa ada seseorang di tengah-tengah mereka yang sedang mengambil data-data tersebut. Gambar 2 mengilustrasikan *Man-in-The-Middle Attack*.



Gambar 2. Ilustrasi *Man-In-The-Middle Attack*

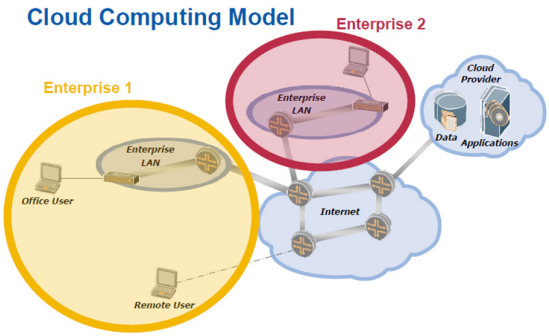
Pada penelitian ini, teknik-teknik keamanan pada *cloud computing* dianalisis dan dibandingkan dalam hal kemampuan menangani ke-empat serangan-serangan keamanan di atas. Teknik-teknik keamanan yang akan diteliti mencakup teknik yang sudah diterapkan di *cloud computing* maupun teknik yang belum diterapkan.

IV. MEKANISME KEAMANAN PADA *CLOUD COMPUTING*

Pada Bab ini akan dijelaskan mekanisme-mekanisme keamanan yang ada pada jaringan *cloud* saat ini dan jaringan *cloud* masa depan (NEBULA).

A. *Current Cloud Computing Network*

Cloud computing yang diimplementasikan saat ini berbasis *address-based* karena bekerja pada jaringan internet yang menggunakan IP *Address* sebagai sarana berkomunikasi. Seperti terlihat pada Gambar 3, setiap perangkat yang terhubung pada *cloud computing* memiliki IP *Address* masing-masing sehingga apabila seorang *user* ingin menghubungi sebuah server yang terdapat di dalam *cloud*, *user* tersebut harus menghubungi IP *Address* dari server tersebut. Arsitektur *Cloud computing* saat ini tidak memungkinkan diimplementasikannya mekanisme-mekanisme keamanan secara fleksibel, oleh karena itu, apabila ada serangan keamanan baru yang muncul, maka mekanisme keamanan yang baru harus diciptakan dan diimplementasikan secara manual ke dalam arsitekturnya [6].

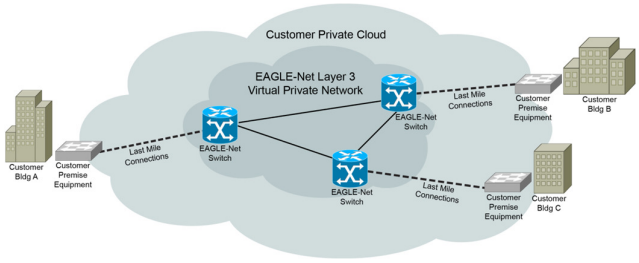


Gambar 3. Mekanisme *Cloud Computing* Saat Ini [6]

Beberapa mekanisme keamanan jaringan yang diterapkan pada *cloud computing* saat ini adalah:

1. VPN (*Virtual Private Network*)

VPN adalah sebuah teknik yang digunakan untuk memastikan bahwa jaringan publik dapat mengakses jaringan privat, dalam kasus ini adalah jaringan *cloud*, secara aman. Gambar 4 berikut mengilustrasikan penggunaan VPN pada jaringan cloud.

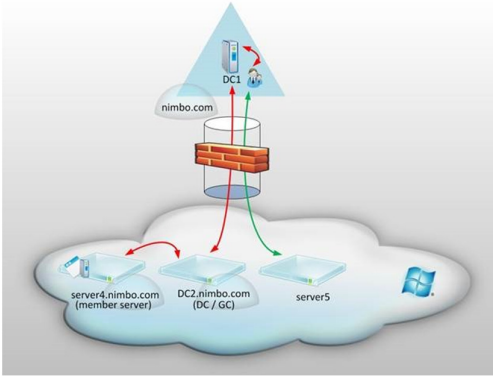


Gambar 4. VPN Pada Jaringan *Cloud* [11]

.

2. *Firewall*

Firewall adalah sebuah mekanisme yang berfungsi untuk memfilter paket-paket data atau *user* yang tidak sesuai dengan kebijakan penyedia *cloud computing*. *Firewall* dapat berupa *software* maupun *hardware*. Dengan melakukan pemfilteran tersebut, *firewall* dapat mencegah serangan dari dalam maupun dari luar jaringan *cloud*. Ilustrasi penggunaan *firewall* pada jaringan *cloud* dapat dilihat pada Gambar 5.



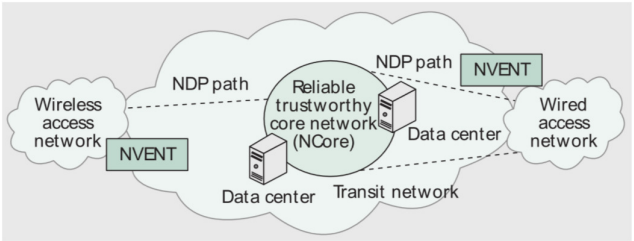
Gambar 5. Ilustrasi *Firewall* Pada *Cloud Computing* [12].

3. Kebijakan dan Konfigurasi Keamanan Pada *Cloud Computing*

Penyedia layanan *cloud computing* dapat menawarkan mekanisme-mekanisme keamanan pada pelanggannya. Mekanisme keamanan ini dikonfigurasi berdasarkan permintaan pelanggan. Contoh mekanisme keamanan yang bisa diimplementasi pada *cloud computing* adalah autentikasi proses dan proses enkripsi-dekripsi [13].

B. NEBULA (*Future Cloud Computing*)

NEBULA adalah sebuah arsitektur jaringan *cloud* masa depan yang bertujuan untuk meningkatkan keamanan dan fleksibilitas dari arsitektur jaringan *cloud* masa kini, salah satu upaya untuk meningkatkan keamanan pada NEBULA adalah mekanisme keamanan yang kuat telah ada di dalam-nya, sehingga apabila muncul serangan keamanan yang baru, maka mekanisme keamanan tersebut dapat beradaptasi secara fleksibel [14]. Arsitektur jaringan NEBULA dapat dilihat pada gambar berikut:



Gambar 6. Arsitektur NEBULA [14].

NEBULA didesain untuk dapat berjalan di jaringan internet sehingga mekanisme keamanan yang ada pada internet juga dapat diimplementasikan di NEBULA. Selain NEBULA dapat diimplementasikan dengan mekanisme keamanan pada internet saat ini, pada NEBULA juga terdapat tiga mekanisme keamanan baru yang bernama *Proof of Path* (PoP), *Proof of Consent* (PoC), dan teknik kriptografi ICING.

Mekanisme keamanan jaringan yang diterapkan pada NEBULA adalah:

1. *Onion Routing*

Onion routing adalah sebuah teknik yang dapat menyembunyikan IP *Address* dari *user*. NEBULA dapat bekerja pada jaringan internet, serta dapat secara fleksibel diimplementasikan mekanisme-mekanisme keamanan, maka *onion routing* dapat diimplementasikan pada NEBULA.

2. *Proof of Path* (PoP)

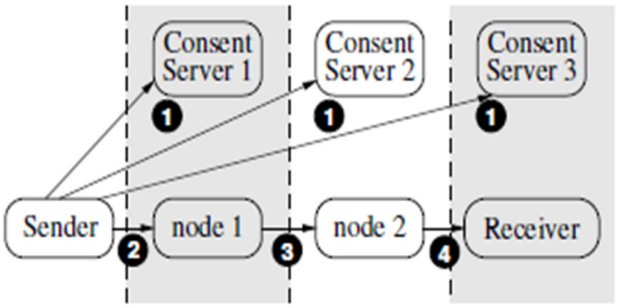
PoP adalah mekanisme yang bertujuan untuk memastikan bahwa jalur yang akan dilalui oleh paket data telah diautentikasi. Dengan demikian, paket-paket akan melewati jalur yang legal sehingga akan mencegah terjadinya banjirnya paket pada jaringan NEBULA, atau disebut *packet flooding* [16].

3. *Proof of Consent* (PoC)

PoC adalah mekanisme yang bertujuan untuk memastikan bahwa *user* dan paket yang akan mengalir di dalam NEBULA telah terautentikasi. Dengan demikian, tidak ada *user* ilegal yang berada di dalam NEBULA, sehingga walaupun ada serangan dari dalam NEBULA maka akan lebih cepat terdeteksi dan diatasi [16].

4. Teknik kriptografi ICING

ICING adalah sebuah teknik kriptografi yang berfungsi untuk melakukan proses enkripsi dan dekripsi pada paket-paket data yang mengalir di dalam NEBULA [17]. Gambar 7 berikut mengilustrasikan skema teknik ICING.



Gambar 7. Ilustrasi Teknik ICING [17].

V. ANALISIS KEAMANAN PADA *CLOUD COMPUTING*

A. *Current Cloud Computing Network*

Penentian kapabilitas keamanan jaringan *cloud computing* saat ini terhadap empat serangan keamanan adalah sebagai berikut:

1. *Snooping attack*

Snooping attack dapat diatasi dengan mekanisme enkripsi-dekripsi yang dapat dikonfigurasi pada jaringan *cloud,* mekanisme enkripsi-dekripsi yang kuat dapat menyembunyikan isi pesan dari *user* yang tidak terautentikasi [15].

2. *Traffic analysis attack*

Penggunaan IP *Address* untuk mengakes setiap perangkat yang berada di dalam *cloud computing* membuat *traffic analysis attack* masih dapat dilakukan pada *cloud computing*, Hal ini dikarenakan seorang penyerang hanya membutuhkan IP *Address* dari target yang akan dia serang untuk melakukan *traffic analysis attack*. Penambahan *onion routing* dapat ditambahkan untuk mengatasi *traffic analysis attack*, namun penambahan *onion routing* tidak fleksibel karena dapat memengaruhi mekanisme lainnya dalam *cloud*.

3. *Denial-of-Service (DoS) attack*

Firewall serta mekanisme *flow control* yang diterapkan pada *cloud computing* dapat mencegah dan mendeteksi gejala awal dari DoS *attack* yaitu munculnya anomali pada jumlah paket data yang mengalir serta munculnya seorang *user* yang tidak terautentikasi yang mencoba untuk memasuki jaringan *cloud*, meskipun demikian, DoS *Attack* masih susah untuk dideteksi [13].

4. *Man-in-the-middle attack*

Mekanisme autentikasi yang kuat perlu diterapkan pada kebijakan konfigurasi *cloud computing* untuk mencegah *man-in-the-middle attack*. Hal ini mengakibatkan *man-in-the-middle attack* tidak secara otomatis dapat diatasi oleh mekanisme yang ada pada *cloud computing*.

Tabel 1 menyimpulkan kapabilitas *cloud computing* dalam mengatasi keempat serangan jaringan tersebut.

Tabel 1. Kapabilitas *Cloud Computing* Dalam Mengatasi Serangan Keamanan

Serangan Keamanan	Mekanisme Keamanan
Snooping	Proses enkripsi-dekripsi paket data
Traffic Analysis	-
Denial of Service	Dengan *Firewall* dan *Flow Control*
Man-in-the-Middle	-

Dari tabel di atas dapat disimpulkan bahwa serangan *traffic analysis* dan *man-in-the-middle* masih dapat dilakukan pada jaringan *cloud*, hal ini dikarenakan mekanisme *cloud computing* yang menganut *address-based* sehingga seorang penyerang hanya perlu mendapatkan IP *Address* dari targetnya yang berada di dalam *cloud* untuk melakukan kedua serangan tersebut. Untuk mencegah terjadinya serangan *man-in-the-middle,* perlu ditambahkan mekanisme autentikasi yang kuat, namun hal ini tidak fleksibel karena akan berdampak pada mekanisme keamanan yang lain [6].

B. NEBULA

Penentian kapabilitas keamanan jaringan *cloud computing* masa depan (NEBULA) terhadap empat serangan keamanan adalah sebagai berikut:

1. *Snooping attack*

Snooping attack dapat diatasi dengan teknik kriptografi ICING yang dapat melakukan mekanisme enkripsi-dekripsi. Teknik kriptografi ICING memungkinkan paket-paket data yang mengalir pada NEBULA tidak bisa terbaca oleh penyerang.

2. *Traffic analysis attack*

Salah satu kelebihan dari NEBULA dibandingkan dengan *cloud computing* adalah tingkat fleksibilitasnya, teknik *onion routing* dapat diimplementasi pada NEBULA, tanpa memengaruhi mekanisme keamanan yang lainnya, dengan tujuan menyembunyikan IP *Address* dari *user*, sehingga *traffic analysis attack* tidak bisa dilakukan.

3. *Denial-of-Service (DoS) attack*

Mekanisme PoC dan PoP pada NEBULA bertujuan untuk mengautentikasi *user*, paket data, serta jalur yang akan dilewati oleh paket data tersebut. Hal ini memungkinkan NEBULA untuk lebih aman dari serangan DoS karena NEBULA akan terhindar dari munculnya anomali pada jumlah paket yang mengalir di dalam NEBULA maupun munculnya *user* yang illegal.

4. *Man-in-the-middle attack*

Mekanisme PoC dan PoP pada NEBULA bertujuan untuk mengautentikasi *user* dan setiap perangkat yang akan berinteraksi melalui NEBULA. Proses autentikasi ini akan mencegah munculnya *user* tidak dikenal sehingga akan mencegah terjadinya serangan *man-in-the-middle*.

Tabel 2 menyimpulkan kapabilitas NEBULA dalam mengatasi keempat serangan jaringan tersebut.

Tabel 2. Kapabilitas NEBULA Dalam Mengatasi Serangan Keamanan

Serangan Keamanan	Mekanisme Keamanan
Snooping	Teknik kriptografi ICING
Traffic Analysis	*Onion Routing*
Denial of Service	PoC dan PoP
Man-in-the-Middle	Poc dan PoP

Dari tabel di atas dapat disimpulkan bahwa NEBULA mampu mengatasi ke-empat serangan keamanan yang diamati. Tiga mekanisme keamanan baru yang diterapkan pada NEBULA, yaitu PoC, PoP, dan teknik kriptografi ICING dapat mencegah munculnya *user* maupun paket data ilegal pada jaringan nebula. Selain itu, tingkat fleksibilitas NEBULA yang tinggi membuat NEBULA mampu dengan cepat mengimplementasikan *onion routing* untuk menyembunyikan IP *address user-user* yang berkomunikasi melalui nebula sehingga dapat mengatasi munculnya *traffic analysis attack*.

Hasil yang didapat pada penelitian ini melengkapi penelitian yang telah dilakukan oleh Rahamatullah et al. [6], di mana review yang dilakukan pada penelitian ini juga membandingkan mekanisme keamanan jaringan masa kini dengna jaringan masa depan.

VI. KESIMPULAN

Beberapa kesimpulan yang dapat dihasilkan dari penelitian ini adalah sebagai berikut:

1. *Cloud computing* saat ini tidak fleksibel karena membutuhkan konfigurasi yang tepat di awal pengimplementasiannya, mekanisme keamanan yang baru perlu diimplementasi secara manual dan akan memengaruhi mekanisme keamanan yang lainnya. NEBULA yang sedang dikembangkan untuk digunakan secara

komplemen dengan *cloud computing* dapat dikonfigurasi sesegera mungkin sehingga lebih fleksibel dalam mengamankan jaringannya.

2. Teknik keamanan yang ada pada *cloud computing* saat ini belum cukup untuk mengatasi seluruh serangan keamanan yang diteliti. Hal ini disebabkan tidak fleksibelnya jaringan *cloud* untuk mengimplementasi mekanisme keamanan, mekanisme keamanan harus terlebih dahulu dikonfigurasi oleh penyedia jaringan *cloud* saat adanya permintaan pelanggan.
3. Teknik keamanan pada nebula, yaitu PoC, PoP, dan ICING dapat mengatasi tiga serangan keamanan yang diteliti, yaitu *snooping attack*, *DoS attack*, dan *man-in-the-middle attack*. Serangan *traffic analysis* dapat diatasi dengan pemakaian *onion routing* yang dapat diimplementasikan dengan cepat pada nebula.

UCAPAN TERIMA KASIH

Ucapan terima kasih diberikan penulis kepada pihak Universitas Mercu Buana Jakarta yang telah memberikan fasilitas penelitian dan juga kepada pihak yang menerbitkan paper ini.

REFERENSI

[1] P. Mell, T. Grance, The NIST Definition of Cloud Computing, Version 15, National Institute of Standards and Technology, 2009, tersedia pada laman situs: http://csrc.nist.gov/groups/SNS/cloud-computing (Diakses pada: 14 Oktober 2015).

[2] Cisco Global Cloud Index: Forecast and Methodology, 2012–2017, tersedia pada laman situs: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html (Diakses pada: 14 Oktober 2015).

[3] Ida Bagus Verry Hendrawan Manuaba, Risanuri Hidayat, dan Sri Suning Kusumawardani. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada). Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), Vol. 1 No. 1, pp 13-17. Mei 2012.

[4] Sugiyanto. Prototipe Sistem Informasi Haji Untuk Menangani Jemaah Tersesat Menggunakan SMS Gateway. Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI). Vol. 03 No. 2, pp 123-128. Mei 2014.

[5] Andrew B. Osmond, Lukito Edi Nugroho, dan Sri Suning Kusumawardhani. Aplikasi Pengumpulan Data Survei Memanfaatkan SMS Gateway. Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), Vol. 5 No. 1, Februari 2016.

[6] Rahamatullah Khondoker, Beny Nugraha, Ronald Marx, and Kpatcha Bayarou. Security Of Selected Future Internet Architectures: A Survey. In *Proceedings of the Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 433-440. July 2014.

[7] Steve Hanna. Cloud Computing: Finding the Silver Lining. Juniper Networks. 2009.

[8] Klöti, Rowan. "Open flow: A security analysis. Master's thesis", Eidgenössische Technische Hochschule Zürich, 2013.

[9] Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher. Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[10] Ciampa, Mark. Security Plus Guide to Network Security Fundamentals. Cengage Learning, 3rd edition, 2009.

[11] EagleNet. Layer 3 Virtual Private Network Service, tersedia pada laman situs: https://www.co-eaglenet.net/services/layer-3-virtual-private-network/ (Diakses pada: Juli 2015).

[12] Bob Hunt. Windows Azure Hybrid Cloud Authentication and Access Architectures, tersedia pada laman situs: http://blogs.technet.com/b/bobh/archive/2013/01/31/windows-azure-hybrid-cloud-authentication-and-access-architectures-discussion-31-days-of-windows-servers-vms-in-the-cloud-part-31-of-31.aspx (Diakses pada: Juli 2015).

[13] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naeslund, dan Makan Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. In International Journal of Cloud Computing: Advances, Systems and Applications. Volume 1, Issue 11. 2012.

[14] Robert Broberg, Matthew Caesar, Douglas Comer, Chase Cotton, Michael J. Freedman, Andreas Haeberlen, Zachary G. Ives, Arvind Krishnamurthy, William Lehr, Boon Thau Loo, David Mazières, Antonio Nicolosi, Jonathan M. Smith, Ion Stoica, Robbert van Renesse, Michael Walfish, Hakim Weatherspoon, dan Christopher S. Yoo. The nebula future internet architecture. Lecture Notes in Computer Science, pages 1–24. Volume 7858, 2013.

[15] Jianli Pan, Subharthi Paul, dan Raj Jain. A survey of the research on future internet architectures. In IEEE Communication Magazine, pages 20–36, July 2011.

[16] Tom Anderson, Ken Birman, Robert Broberg, Matthew Caesar, Douglas Comer, Chase Cotton, Michael Freedman, Andreas Haeberlen, Zack Ives, Arvind Krishnamurthy, William Lehr, Boon Thau Loo, David Mazières, Antonio Nicolosi, Jonathan Smith, Ion Stoica, Robbert van Renesse, Michael Walfish, Hakim Weatherspoon, dan Christopher Yoo. Technical report. nebula - a future internet that supports trustworthy cloud computing. Pages 1–31, 2011.

[17] Jad Naous, Michael Walfish, Antonio Nicolosi, David Mazieres, Michael Miller, and Arun Seehra. Verifying and enforcing network paths with ICING, in Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies (CoNEXT 2011), Article No. 30, 2011.