Jurnal Sistem Informasi (JSI), VOL. 8, NO. 1, April 2016,
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

ANALISIS KERENTANAN DAN KEHANDALAN LAYANAN JARINGAN CLOUD BERBASIS PLATFORM EUCALYPTUS

Yudhi Kusnanto
Teknik Komputer, STMIK Akakom Yogyakarta
Email: yudhi@akakom.ac.id

Abstract

Cloud computing is a computing paradigm that evolves from existing technology, such as grid computing, virtualization and the Internet. Cloud computing provides an illusion of unlimited computing resources, which can be accessed from anywhere, anytime. Despite the potential gains achieved from the cloud computing, the model security is still questionable which hindered adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. Eucalyptus-based cloud network services widely deployed as private cloud infrastructure. Experiment on this paper focused on finding potential denial-of-service (DOS) and the impact on ability to provide services during attack. We observe an increase on response time up to 2863.22% during attack to the web-based management service. Reducing average system load to an acceptable level, help prevents disruption of the service, by implementing rate control and rate limit on cloud controller.

Keywords: cloud computing, network security, operating system, Eucalyptus

Abstrak

Cloud computing adalah sebuah teknologi yang mampu memberi ilusi sumber daya komputasi yang tak terhingga, yang dapat diakses dari mana saja, kapan saja. Meskipun cloud computing berpotensi memberikan manfaat yang besar, namun masalah keamanannya masih menjadi pertanyaan, yang mana menghambat adopsi-nya. Persoalan keamanan pada cloud computing menjadi semakin rumit karena karakteristik cloud computing yang khas seperti kelenturan alokasi sumber daya, dan pengguna yang jamak. Jaringan cloud berbasis platform Eucalyptus banyak diterapkan pada fasilitas cloud privat. Penelitian ini bertujuan untuk mengetahui potensi hambatan atas pelayanan jaringan cloud akibat serangan yang terarah (targeted attack), pada sistem jaringan cloud berbasis platform Eucalyptus. Pengujian menunjukkan adanya peningkatan waktu respons hingga 2863,22% akibat serangan terarah terhadap layanan web administrasi. Penerapan pembatasan dan kendali laju data (rate control, rate limit) pada penelitian ini merupakan solusi untuk mengurangi dampak serangan terarah. Dengan langkah mitigasi ini peningkatan beban dapat dikendalikan sehingga tidak memengaruhi pelayanan. Pengujian kerentanan menunjukkan layanan jaringan cloud berbasis platform Eucalyptus tidak memiliki ancaman kerentanan yang berpotensi menjadi serangan keamanan.

Kata kunci: cloud computing; keamanan jaringan, sistem operasi, Eucalyptus

1. Pendahuluan

Teknologi *Cloud Computing* adalah suatu paradigma dalam teknologi komputasi yang merupakan konvergensi dari teknologi komputasi tersebar (*distributed computing*), *grid computing*, virtualisasi, Internet dan teknologi Web 2.0 yang semakin berkembang beberapa tahun ini [1]. Teknologi ini menawarkan beragam manfaat, misalnya sumber daya komputasi yang dapat dimanfaatkan sesuai permintaan (*on-demand*). Data-data yang tersimpan pada sistem cloud dapat diakses dari manapun, kapanpun dan dari perangkat apapun sepanjang terdapat sambungan dengan Internet.

Namun demikian persoalan keamanan dan privasi pada cloud computing masih menjadi pertanyaan yang perlu dijawab dengan memuaskan karena akan mempengaruhi penerimaan masyarakat. Persoalan menjadi semakin rumit karena arsitektur cloud computing

memungkinkan banyak penghuni (*multi-tenancy*), kelenturan alokasi sumber daya (elasticity) dan susunan layanan yang bertingkat (*inter-service dependency stack*) [2]. Penelitian ini dilakukan untuk mengkaji berbagai persoalan yang berkaitan dengan keamanan layanan jaringan pada sistem *cloud*: a) Mengidentifikasi ancaman keamanan dalam sistem *cloud computing* yang berbasis platform EUCALYPTUS; b) Menetapkan prosedur mitigasi untuk mengurangi kerugian saat mengalami serangan.

2. Infrastruktur Jaringan Cloud Berbasis Platform Eucalyptus

A. Penelitian Sebelumnya

Kajian oleh Jadeja & Modi [3] memberikan gambaran mengenai teknologi *cloud computing* serta tantangan yang dihadapi. Penelitian yang dilakukan oleh Popović & Hocenski [4], Morsy, Grundy & Müller [2], Wang [5] menunjukkan aspek-aspek keamanan dan privasi yang perlu diperhatikan dalam layanan *cloud computing*. Pembahasan ditinjau dari sudut pandang kepentingan pengguna dan penyedia jasa. Tanimoto dkk [6] membahas keamanan jaringan *cloud* dalam rangka manajemen risiko. Szefer, Jamkhedkar, Chen & Lee [7] menawarkan model perlindungan fasilitas pusat data (*data center*) secara fisik dan virtual berdasarkan sensor fisik dan sensor *cyber*.

B. Arsitektur Keamanan Jaringan

International Telecommunication Union (ITU) *Telecommunication Standardization Sector* (ITU-T) dalam rekomendasi ITU-T X.800 [8] memberikan batasan istilah "keamanan" dalam arti mengurangi kerentanan dari suatu aset dan sumber daya. Aset adalah segala sesuatu yang memiliki nilai (*value*). Kerentanan adalah setiap kelemahan yang dapat di-eksploitasi sehingga mengganggu sistem atau informasi yang terdapat di dalam sistem. Ancaman diartikan sebagai suatu potensi yang dapat mengganggu keamanan.

Secara umum, hal-hal berikut memerlukan perlindungan:

- Informasi dan data (termasuk perangkat lunak dan *password*);
- Layanan komunikasi dan pengolahan data; dan
- Peralatan dan fasilitas.

Rekomendasi ITU-T X.805 [9] membahas tentang arsitektur keamanan jaringan untuk urusan manajemen, pengendalian dan pemanfaatan atas infrastruktur, layanan dan aplikasi jaringan. Arsitektur keamanan membagi secara logis fitur-fitur keamanan jaringan yang kompleks menjadi komponen terpisah, yaitu: Dimensi keamanan (*security dimensions*); Lapis keamanan (*security layers*); dan Bidang keamanan (*security planes*).

1. Dimensi keamanan

   Dimensi keamanan adalah sejumlah langkah-langkah pengamanan yang dirancang untuk mengatasi aspek tertentu dalam masalah keamanan jaringan. Terdapat delapan dimensi keamanan menurut ITU-T X.805, yaitu: *Access control*; *Authentication*; *Non-repudiation*; *Data confidentiality*; *Communication security*; *Data integrity*; *Availability*; dan *Privacy*.

2. Lapis keamanan

Dimensi keamanan perlu diterapkan ke dalam suatu hierarki peralatan jaringan yang disebut lapis keamanan. Lapis keamanan didefinisikan menjadi tiga macam, yaitu: Lapisan Infrastruktur (*Infrastructure Layer*); Lapisan Layanan (*Services Layer*), dan Lapisan Aplikasi (*Application Layer*). Lapis keamanan merupakan serangkaian solusi yang memungkinkan jaringan yang aman, sedemikian rupa sehingga lapisan infrastruktur memungkinkan lapisan layanan, dan lapisan layanan memungkinkan lapisan aplikasi. Hal ini karena setiap lapis keamanan memiliki kerentanan keamanan yang berbeda.

3. Bidang keamanan

   Bidang keamanan adalah jenis aktivitas tertentu dalam jaringan yang dilindungi oleh dimensi keamanan. Ada tiga bidang yang dilindungi, yaitu: Bidang Manajemen (*Management Plane*), Bidang Kendali (*Control Plane*), dan Bidang Pengguna (*End-user Plane*).

C. Ancaman Keamanan

Aspek keamanan akan meningkatkan biaya dan menambah kerumitan dalam pemanfaatannya. Oleh karena itu perlu dilakukan identifikasi atas setiap ancaman agar diketahui jenis perlindungan yang diperlukan dan memberikan keseimbangan dengan kemudahan penggunaannya. Suatu sistem memiliki kerentanan dalam berbagai bentuk namun tidak semuanya dapat di-eksploitasi menjadi serangan. Hal ini karena si penyerang tidak memiliki kesempatan atau hasil yang diperoleh tidak sebanding dan risiko terdeteksi [8]. Ancaman pada sistem komunikasi data (termasuk jaringan komputer) adalah:

- Penghancuran informasi atau sumber daya lainnya;
- Perusakan atau pengubahan/modifikasi informasi;
- Pencurian, penghilangan informasi dan/atau sumber daya lainnya;
- Pengungkapan informasi; dan
- Penghentian layanan.

Ancaman dapat terjadi karena kesengajaan (*intentional*) misal, mencari kelemahan kemudian mengeksploitasi-nya; atau kecelakaan (*accidental*) misal, *software bugs* dan *hardware failure;* dan dapat dilakukan secara aktif (mengubah, mengganti, merusak informasi) atau pasif (menyadap, *surveillance*, analisis trafik).

D. Strategi Pertahanan

Tindakan pengamanan memerlukan biaya dan berakibat berkurangnya kemudahan pemanfaatan sistem. Semakin tinggi tingkat keamanan yang diterapkan, semakin sulit pemanfaatannya. Oleh karena itu perlu dilakukan kajian untuk menyeimbangkan antara tingkat keamanan dan tingkat kemudahan atas suatu aset sesuai dengan nilai kepentingan aset tersebut dan biaya yang ada. Upaya non-teknis seperti perlindungan asuransi, kadang kala merupakan alternatif yang lebih murah dibanding pengamanan teknis semata.

E. Mitigasi

Persoalan keamanan jaringan tidak saja mempertimbangkan pencegahan dan pertahanan, melainkan juga perlu mempersiapkan langkah-langkah mitigasi. Mitigasi diartikan sebagai

tindakan untuk mengurangi kerugian. Hal ini dengan kesadaran bahwa setiap gangguan selalu berakibat kerugian baik dalam bentuk material/finansial maupun bentuk yang lain. Langkah mitigasi diambil sesuai dengan jenis ancaman yang terjadi sebagaimana disajikan dalam Tabel 1:

Tabel 1: Strategi mitigasi terhadap ancaman

Ancaman	Mitigasi
Penghancuran informasi atau sumber daya lainnya	cadangan alternatif, baik untuk informasi maupun sumber daya lain
Perusakan atau pengubahan (modifikasi) informasi	
Pencurian, penghilangan informasi dan/atau sumber daya lainnya	enkripsi, asuransi, *asset tracking*
Pengungkapan informasi	*logging*, kendali akses
Penghentian layanan (*denial-of-service*, DoS)	*re-route*, alternatif saluran

F. *Cloud Computing*

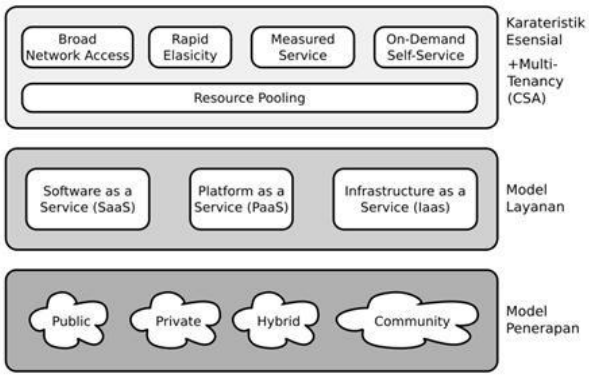
The National Institute of Standards and Technology (NIST), suatu badan pemerintah Amerika Serikat, memberikan definisi *cloud computing* yang diuraikan ke dalam lima karakteristik esensial, tiga model layanan dan empat model penerapan [10], yaitu:

1. Karakteristik esensial
    a. *On-demand self-service.*
    b. *Broad network access*
    c. *Resource pooling.*
    d. *Rapid elasticity.*
    e. *Measured service.*
2. Model layanan
    a. *Software-as-a-Service* (SaaS).
    b. *Platform-as-a-Service* (PaaS).
    c. *Infrastructure-as-a-Service* (IaaS).
3. Model penerapan
    a. *Public Cloud*.
    b. *Private Cloud*.
    c. *Community Cloud*.
    d. *Hybrid Cloud*.

Cloud Security Alliance (CSA) menambahkan sebuah karakteristik yang dianggap esensial dalam sistem *cloud* [11], yaitu: *Multi-Tenancy*. Layanan *cloud* memungkinkan banyak konsumen yang berbeda memanfaatkan infrastruktur yang sama.

Gambar 1 menampilkan visualisasi definisi *cloud computing*. Berdasarkan definisi tersebut, pengertian *cloud computing* dapat disimpulkan sebagai suatu model layanan yang memungkinkan akses ke suatu sumber daya komputasi sesuai keperluan, mudah digunakan, yang dengan cepat dapat difungsikan atau dihentikan, tanpa perlu berinteraksi dengan penyedia layanan.

Jurnal Sistem Informasi (JSI), VOL. 8, NO. 1, April 2016,
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com



Gambar 1: Visualisasi definisi cloud computing

G. Platform Eucalyptus

Eucalyptus [12] merupakan suatu perangkat lunak berbasis Linux yang mengimplementasikan *private* dan *hybrid cloud* ke dalam infrastruktur teknologi informasi yang ada. Eucalyptus memungkinkan penyiapan semua sumber daya yang dimiliki (*hardware*, *storage* dan *network*) secara swalayan sesuai keperluan. Eucalyptus dapat diterapkan pada jaringan pusat data di lingkungan sendiri (*on-premise data center*), dimana pengguna mengakses layanan melalui jaringan intranet.

1. Komponen

   Platform Eucalyptus tersusun atas enam komponen. Hal ini dirancang agar penerapan sistem Eucalyptus menjadi lebih fleksibel mengikuti berbagai konfigurasi pusat data yang ada. Ke-enam komponen tersebut adalah: **Cloud Controller** (CLC), **Walrus**, **Cluster Controller** (CC), **Storage Controller** (SC), **Node Controller** (NC) dan sebagai pilihan, **VMware Broker** (**Broker** atau VB). Selain **VMware Broker**, setiap komponen merupakan layanan web (*web service*) yang mandiri. Ilustrasi susunan komponen Eucalyptus seperti yang ditampilkan pada Gambar 2.

Gambar 2: Komponen Eucalyptus [13]

2. Mode operasi
   - **Managed Mode**. Eucalyptus mengelola jaringan lokal dari semua *VM instances* dan menyediakan semua fitur yang ada, yaitu *VM network isolation*, *security groups*, *elastic IP*, dan layanan metadata.
   - **Managed (No VLAN) Mode**. Eucalyptus mengelola jaringan lokal dari semua *VM instances* dan menyediakan semua fitur *security groups*, *elastic IP* dan layanan metadata, kecuali *VM network isolation*. Hal ini memungkinkan *root user* dari satu *VM instance* mengganggu trafik ethernet VM lain yang terhubung dengan *switch* yang sama.

- **System Mode**. Eucalyptus hanya memberi alamat MAC untuk *VM instance* tanpa alamat IP. Alamat IP untuk *VM instance* diperoleh dari *server* DHCP yang ada di dalam jaringan. Kekurangannya adalah tiadanya fitur *VM network isolation*, *security groups* dan *elastic IP*.
- **Static Mode**. Sejenis dengan mode System namun alamat IP untuk *VM instance* ditetapkan secara statis pada *server* DHCP yang dikelola Eucalyptus.

3. Fitur berjaringan

   Eucalyptus dapat dibangun di atas instalasi jaringan komputer yang telah ada atau berdiri sendiri. Pertimbangan pemilihan mode operasi didasarkan pada fitur-fitur yang diinginkan. Tabel 2 menunjukkan fitur-fitur yang disediakan oleh Eucalyptus.

Tabel 2: Fitur berjaringan Eucalyptus

Fitur	Uraian	Mode
Elastic IP	Sekumpulan alamat IP yang ditetapkan dapat diberikan pada setiap VM instance secara dinamis. Dengan demikian pengguna dapat menjalankan layanan dalam sistem cloud.	Managed Managed (No VLAN)
Security-groups	Sekumpulan tata-aturan yang mengatur akses ke setiap VM *instances* yang tergabung dalam satu kelompok. Dalam keadaan default, akses ke VM instance dari jaringan adalah ditolak. Untuk membuka akses jaringan, digunakan perintah **euca-authorize**.	Managed Managed (No VLAN)
VM isolation	Trafik jaringan antar VM instances dalam satu kelompok keamanan (security group) yang sama selalu terbuka. Eucalyptus dapat memisahkan trafik jaringan dari kelompok keamanan yang berbeda, dengan memberikan tag VLAN yang berbeda. Dengan fitur ini, dapat dicegah adanya penyadapan oleh pihak lain meskipun masih dalam hypervisor yang sama.	Managed
DHCP server	Pemberian alamat IP pada mode System, dilakukan oleh DHCP server yang ada di jaringan.	Static Managed Managed (No VLAN)

4. Antarmuka manajemen

   Pengelolaan platform *cloud* merupakan kegiatan yang penting agar diperoleh kinerja yang optimal. Semua layanan pengelolaan disediakan oleh CLC yang tidak saja menyajikan informasi mengenai sistem *cloud* namun juga memberikan layanan untuk mengelola semua sumber daya *cloud* (*server*, *storage* dan *network*).

   - *Web-based Management Console* (WBMC). Dengan layanan berbasis web, pengguna cukup menjalankan aplikasi penjelajah web (*web browser*) untuk melakukan pengelolaan *cloud*.
   - *Command-line Interface* (CLI). Eucalyptus juga menyediakan layanan yang dapat diakses secara programatik. Layanan CLI diakses menggunakan program aplikasi khusus yang telah disediakan.

H. Sistem Operasi KALI Linux

Untuk melakukan pengujian keamanan sistem secara sistematis dan otomatis, telah tersedia distribusi Linux yang khusus dibangun untuk keperluan itu. Distribusi tersebut adalah Kali Linux yang dikembangkan oleh komunitas penggiat masalah keamanan dan tersedia

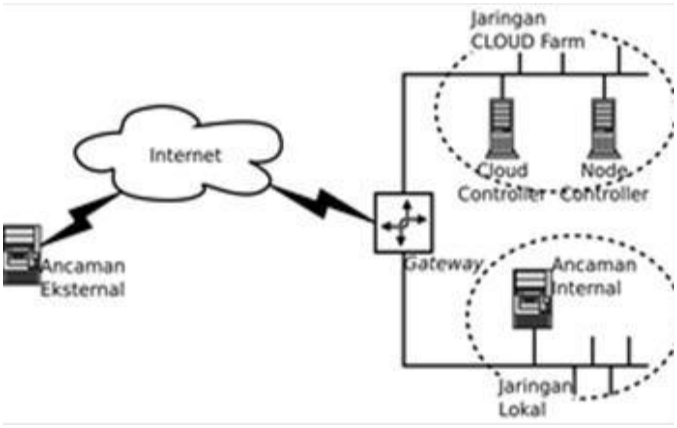
bebas di Internet. Kali Linux mengandung aplikasi-aplikasi yang bermanfaat untuk berbagai keperluan pengujian sistem, antara lain adalah aplikasi **wireshark, OpenVAS** dan **zenmap**. Aplikasi lainnya dikelompokkan ke dalam beberapa kategori/menu yaitu *Information Gathering*; *Vulnerability Analysis*; *Web Applications*; *Password Attacks*; *Wireless Attacks*; *Exploitation Tools*; *Sniffing/Spoofing*; *Maintaining Access*; *Reverse Engineering*; *Stress Testing*; *Hardware Hacking*; *Forensic Tools*; dan *Reporting Tools*.

Dalam suatu sistem operasi terdapat aplikasi untuk keperluan administrasi dan pengelolaan sistem. Aplikasi ini dapat dimanfaatkan sebagai alat yang efektif untuk tugas pengujian sistem. Salah satu aplikasi untuk pemeliharaan sistem operasi adalah **sar**. **sar** merupakan suatu program bantu untuk mengumpulkan dan merekam data-data unjuk-kerja yang dihasilkan oleh *kernel* sistem operasi. Data tersebut dapat disajikan langsung di layar monitor atau disimpan ke dalam suatu berkas untuk analisis lebih lanjut. Aplikasi lainnya adalah **wget** yaitu program untuk mengunduh data (objek) dari Internet dan menyimpannya langsung ke komputer menggunakan protokol HTTP.

3. Perancangan Dan Implementasi *Test-bed*

A. Rancangan Arsitektur Jaringan

Secara ideal rancangan arsitektur jaringan *cloud* dalam penelitian ini seperti ditunjukkan pada Gambar 3.



Gambar 3: Diagram umum jaringan test-bed

Sistem Eucalyptus disusun dalam konfigurasi menggunakan dua unit *server*, satu unit sebagai *Cloud Controller* (CLC) sedangkan lainnya sebagai *Node Controller* (NC). CLC merupakan "beranda" dari sistem *cloud* dan wajib memiliki sambungan dengan Internet sementara NC cukup memiliki sambungan dengan CLC (CC) melalui jaringan privat.

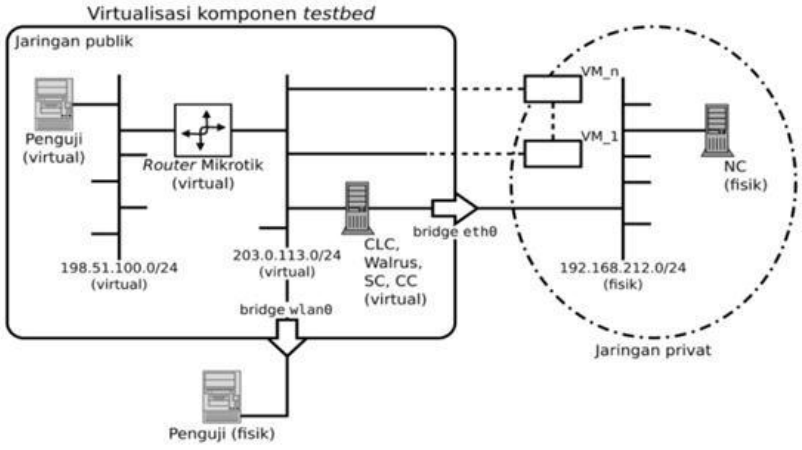
B. Skenario Pengujian

Dalam penelitian ini, pengujian diterapkan pada lapis infrastruktur jaringan *cloud* yang berbasis Eucalyptus. Dengan demikian model-model ancaman yang tidak relevan terhadap operasional sistem *cloud* sengaja ditinggalkan. Secara *default*, sistem Eucalyptus telah memiliki fitur pertahanan yang dapat mencegah beberapa jenis ancaman seperti penerapan enkripsi pada layanan manajemen, penghalangan/penyaringan (*blocking/filtering*) paket data

Jurnal Sistem Informasi (JSI), VOL. 8, NO. 1, April 2016,
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com

yang menuju ke VM *instances* dan pemisahan jaringan secara virtual untuk setiap kelompok VM dengan menerapkan VLAN *tagging* (dalam mode MANAGED).

Realisasi infrastruktur *test-bed* diwujudkan dalam kombinasi peralatan fisik dan pemanfaatan teknologi virtualisasi. Hal ini merupakan siasat (*workaround*) untuk mengatasi kekurangan peralatan yang diperlukan dalam pengujian. Bagian yang diwujudkan secara fisik adalah NC dan sambungannya ke CLC (jaringan privat), sedangkan konstelasi jaringan publik (CLC, *router*, penguji, LAN) diwujudkan dengan memanfaatkan teknologi virtualisasi pada sebuah komputer, seperti ditunjukkan pada Gambar 4.



Gambar 4: Realisasi jaringan publik dalam test-bed

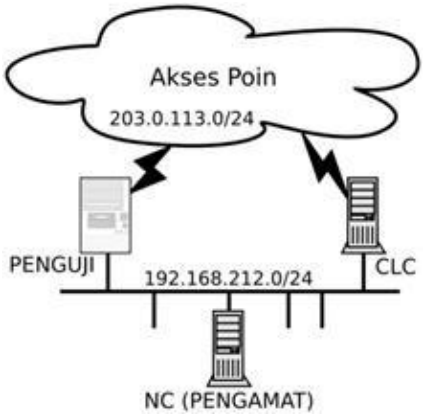
1. Uji kerentanan

   Pengujian untuk mengidentifikasi celah-celah keamanan sistem *cloud* dari luar fasilitas. Percobaan ini didasarkan pada riwayat yang tercatat pada basis-data kerentanan (*vulnerability database*). Sasarannya adalah lapisan infrastruktur (*infrastructure layer*), lapisan layanan (*services layer*) dan lapisan aplikasi (*applications layer*) dalam sistem *cloud*..

2. Uji kehandalan layanan web administrasi

   Ancaman terhadap sistem *cloud* tidak saja yang berdampak pada kerusakan atau kebocoran informasi namun juga terhentinya layanan akibat serangan. Hal ini merupakan salah satu indikator kualitas layanan yang disediakan, yaitu jaminan ketersediaan layanan. Pengujian kehandalan ditujukan untuk mengetahui potensi *denial-of-services* (DoS) atas layanan yang disediakan yaitu layanan web, *port* 8443/HTTPS. Pemasangan layanan HTTPS memanfaatkan teknik SSL sehingga setiap komunikasi dengan pengguna/klien akan meningkatkan beban *server*. Untuk pengujian ini, jaringan *cloud* tidak diwujudkan dalam model virtualisasi, namun dalam konfigurasi fisik seluruhnya. Diagram jaringan untuk pengujian ini ditunjukkan pada Gambar 5.

Jurnal Sistem Informasi (JSI), VOL. 8, NO. 1, April 2016,
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com



Gambar 5: Diagram untuk pengujian kehandalan

Pengujian dilakukan dengan menggunakan perangkat **thc-ssl-dos** [14] yang telah dimodifikasi untuk keperluan pengujian pada penelitian ini. Modifikasi dilakukan untuk memberi pilihan lama pengujian (dalam detik), dan dapat menampilkan tanda-waktu (*time-stamp*) untuk kemudahan analisis. Variasi serangan dilakukan dengan mengubah waktu/lama serangan dan jumlah penyerang. Pengukuran waktu respons layanan dilakukan di NC yaitu dengan mencatat total waktu yang diperlukan untuk mengambil semua objek pada halaman awal (*login page*) termasuk gambar-gambar dan skrip web (Javascript dan CSS). Perangkat untuk pengamatan menggunakan program **wget** sedangkan pengukur waktunya memanfaatkan fasilitas yang tersedia dalam *shell* Bash. Skrip pengujian menggunakan bahasa pemrograman *shell* Bash, baik untuk pengendalian, penyerangan maupun pengamatan. Sinkronisasi isyarat dilakukan dengan semafor dengan acuan waktu yang diberikan oleh penyerang.

4. Hasil Pengujian Dan Analisis

A. Pengujian Operasional

1. Koneksi jaringan

   Pengujian koneksi dilakukan dengan menjalankan program **ping** dan **traceroute** dari CLC dan Penguji ke NC serta sebaliknya. Status keluaran masing-masing program menandakan adanya koneksi dan kesiapan infrastruktur jaringan.

2. Pengujian sistem Eucalyptus

   Sistem cloud Eucalyptus mendefinisikan pelanggannya sebagai "**Account**" dan di dalamnya terdapat beberapa "**User**". Secara default, instalasi Eucalyptus akan membuat account **eucalyptus** dan user **admin**. Akun ini merupakan akun untuk keperluan administrasi sistem *cloud* secara keseluruhan. Untuk keperluan non-administratif (penggunaan layanan), perlu dibuat akun lainnya. User admin secara otomatis dibuat setiap kali sebuah akun diaktifkan. User admin inilah yang digunakan ketika masuk ke dalam sistem cloud. Password yang diisi-kan pada saat pendaftaran, melekat pada user admin.

Layanan web administrasi digunakan untuk mengetahui dan mengelola akun. Selain itu,

juga digunakan untuk membuat kunci akses ke dalam sistem cloud secara programatik. Kunci berupa sertifikat ini, akan digunakan untuk menyandikan saluran komunikasi dengan server dan otorisasi akses.

B. Pengujian Kerentanan

1. Pengumpulan informasi

   Layanan yang tersedia pada CLC relatif sedikit dan sebagian besar diatur hanya melayani internal cloud. Hanya layanan SSH (remote access) dan web pada port TCP/8443/HTTPS yang aktif untuk publik (layanan HTTP pada port TCP/8080 akan mengalihkan permintaan ke layanan TCP/8443/HTTPS). Tabel 3 menunjukkan layanan-layanan yang terdeteksi pada CLC.

2. Potensi kerentanan

   Layanan web pada port 8443/HTTPS dibangun memanfaatkan program yang telah tersedia dalam bahasa Java, yaitu Mortbay Jetty versi 6.1.x. Dalam catatan kerentanan pada perangkat OpenVAS Vulnerability Scanner ini, produk Mortbay Jetty versi 6.1.x memiliki kekeliruan pada instalasi default-nya yaitu ikut memasang kode demonstrasi sehingga dapat diakses oleh publik.

   Instalasi program Mortbay Jetty versi 6.1.x yang dilakukan oleh Eucalyptus tidak memasang kode yang bermasalah tersebut. Dengan demikian peringatan yang disampaikan oleh OpenVAS tidak relevan untuk sistem Eucalyptus (false-negative).

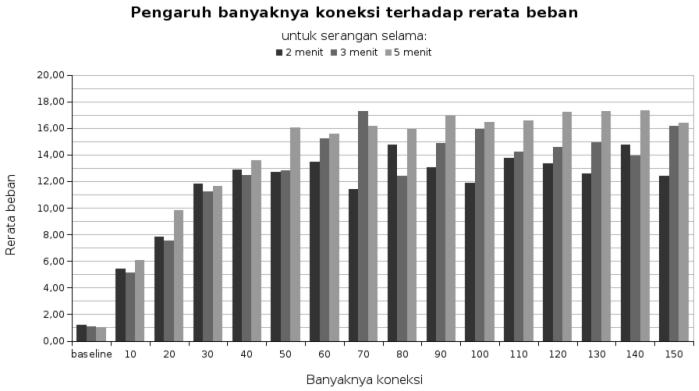
Tabel 3: Hasil identifikasi layanan di CLC

host	port	protokol	layanan	informasi
203.0.113.2	22	tcp	ssh	SSH-2.0-OpenSSH_5.3
203.0.113.2	8080	tcp	http	Jetty 6.1.x
203.0.113.2	53	tcp	domain	-tak-dikenal-
203.0.113.2	3260	tcp	tcpwrapped	-tak-dikenal-
203.0.113.2	5000	tcp	vtun	Vtun Virtual Tunnel 3.X 07/08/2010
203.0.113.2	8443	tcp	http	Jetty 6.1.x
203.0.113.2	8888	tcp	hadoop-tasktracker	Apache Hadoop 2.2.1
203.0.113.2	53	udp	domain	-tak-dikenal-
203.0.113.2	8773	tcp	http	-tak-dikenal-
203.0.113.2	8774	tcp		-tak-dikenal-

C. Pengujian Kehandalan Layanan Web

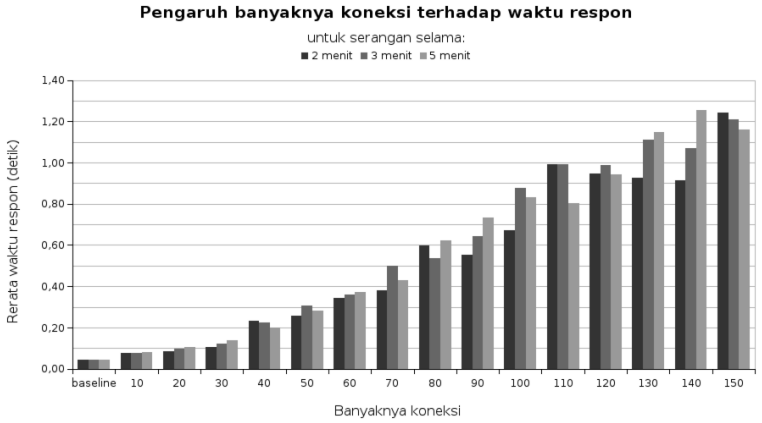
Kehandalan sistem *cloud* secara langsung ditentukan oleh ketersediaan layanan web administrasi dan manajemen. Dalam hal ini, serangan apapun yang dapat menyibukkan *server* dan menghabiskan sumber daya akan berpotensi meniadakan pelayanan. Pengujian kehandalan layanan web dilakukan dengan mengeksploitasi koneksi HTTPS pada *port* 8443/TCP. Eksploitasi tersebut melakukan koneksi terus-menerus, sebanyak-banyaknya, sehingga sistem *cloud* akan kehabisan sumber daya. Pada akhirnya tidak dapat memberi pelayanan kepada pengguna. Grafik pada Gambar 6 memperlihatkan kecenderungan peningkatan beban kerja seiring meningkatnya jumlah koneksi (penyerang).

Jurnal Sistem Informasi (JSI), VOL. 8, NO. 1, April 2016,
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com



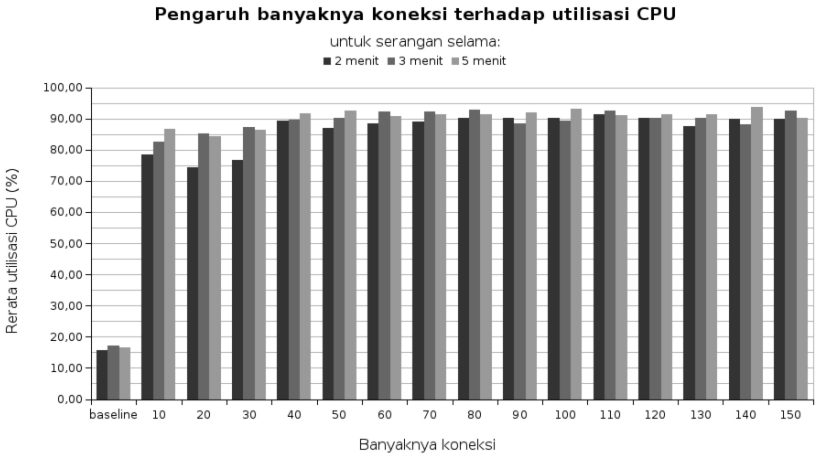
Gambar 6: Rerata beban di CLC

Semakin banyak koneksi, semakin meningkat rerata beban. Namun demikian, tidak terlihat perbedaan yang signifikan akibat perbedaan waktu serangan. Waktu respons yang dialami oleh pengguna, ikut mengalami peningkatan seiring meningkatnya jumlah koneksi, seperti ditunjukkan pada Gambar 7.



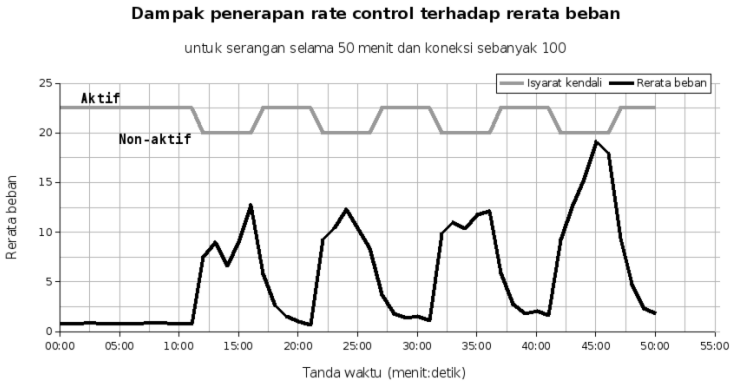
Gambar 7: Rerata waktu respon layanan

Hasil ini menunjukkan bahwa peningkatan waktu respons dipengaruhi juga oleh banyaknya koneksi. Utilisasi CPU merupakan indikator kesibukan sistem untuk mengerjakan tugas-tugas komputasi numeris. Dalam hal ini diperlukan untuk mengolah algoritma enkripsi. Grafik pada Gambar 8 menunjukkan adanya peningkatan utilisasi seiring meningkatnya jumlah koneksi.



Gambar 8: Rerata utilisasi CPU pada CLC

Jurnal Sistem Informasi (JSI), VOL. 8, NO. 1, April 2016,
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsi.fasilkom.unsri@gmail.com



Gambar 9: Rerata beban dalam penerapan rate control

Mitigasi dengan menerapkan mekanisme pembatasan dan pengaturan laju data (*rate control, rate limiter*) pada *port* TCP/8443/HTTPS [15], dapat mengurangi pengaruh serangan, yaitu penurunan nilai rerata beban. Visualisasi rerata beban dalam penerapan mitigasi ditunjukkan pada Gambar 9. Hasil pengujian pada Tabel 4 menunjukkan bahwa lama serangan tidak berpengaruh signifikan terhadap peningkatan waktu respons namun sebaliknya justru dipengaruhi oleh jumlah koneksi. Hal ini ditunjukkan dengan nilai simpangan baku dari ketiga jenis serangan yang relatif kecil [16]. Sementara itu, tampak pula peningkatan waktu respons yang mencapai hingga 2863,22% dari *baseline* seiring bertambahnya jumlah koneksi. Akibatnya kenyamanan pengguna terganggu saat menggunakan layanan *cloud*.

5. Kesimpulan

Penelitian ini menunjukkan beberapa kesimpulan sehubungan dengan pemasangan dan instalasi sistem cloud berbasis platform Eucalyptus, yaitu:

1. Sistem Eucalyptus memberikan perlindungan keamanan untuk penerapan sistem cloud dalam lingkungan privat, yaitu: (a) adanya enkripsi untuk setiap komunikasi; (b) adanya penyaringan untuk setiap lalu-lintas data (packet filtering) ke jaringan VM; dan (c) memisahkan jaringan lokal untuk cluster dan node-controller dari jaringan publik.
2. Faktor yang memengaruhi peningkatan rerata waktu respons ditentukan oleh banyaknya koneksi secara bersamaan dibanding lamanya serangan. Hal ini karena simpangan baku atas perbedaan lamanya serangan relatif kecil yaitu antara 0,0019 detik dan 0,1712 detik.

Tabel 4: Rerata waktu respons layanan web

Banyak Koneksi	Serangan 2 menit		Serangan 3 menit		Serangan 5 menit		Stddev (detik)
	Waktu respons (detik)	Kenaikan terhadap *baseline*	Waktu respons (detik)	Kenaikan terhadap *baseline*	Waktu respons (detik)	Kenaikan terhadap *baseline*	
baseline	0,044	-	0,042	-	0,042	-	0,0008
10	0,078	78,68%	0,076	80,72%	0,080	88,79%	0,0019
20	0,086	96,31%	0,095	126,10%	0,106	151,17%	0,0104
30	0,105	141,59%	0,124	194,11%	0,139	229,10%	0,0170
40	0,232	430,97%	0,225	433,22%	0,199	370,57%	0,0170
50	0,259	494,08%	0,308	631,37%	0,282	565,30%	0,0245
60	0,344	687,98%	0,361	757,86%	0,373	779,86%	0,0145
70	0,380	771,22%	0,501	1088,39%	0,432	919,48%	0,0605
80	0,596	1267,42%	0,537	1174,11%	0,622	1368,19%	0,0436
90	0,555	1171,84%	0,641	1422,23%	0,731	1627,62%	0,0884
100	0,670	1435,26%	0,878	1985,05%	0,833	1867,96%	0,1098
110	0,993	2177,24%	0,991	2251,82%	0,802	1794,51%	0,1096
120	0,945	2066,59%	0,986	2239,93%	0,944	2129,50%	0,0238
130	0,927	2024,70%	1,112	2539,05%	1,149	2614,45%	0,1192
140	0,913	1992,07%	1,071	2442,48%	1,255	2863,22%	0,1712
150	1,242	2748,52%	1,209	2769,92%	1,160	2638,97%	0,0416

DAFTAR PUSTAKA

[1] Menascé D. & Ngo P., Understanding cloud computing: experimentation and capacity planning. In *Proc. 2009 Computer Measurement Group's Intl. Conf.*. 2009.
[2] Morsy MA., Grundy J. & Müller I., An analysis of the cloud computing security problem. In *Proc. of APSEC 2010 Cloud Workshop, Sydney, Australia*. 2010.
[3] Jadeja Y. & Modi K., Cloud computing - concepts, architecture and challenges. In *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*. 2012.
[4] Popović K. & Hocenski Ž., Cloud computing security issues and challenges. In *MIPRO, 2010 Proceedings of the 33rd International Convention, Opatija, Croatia*. 2010.
[5] Wang Z., Security and privacy issues within the cloud computing. In *Computational and Information Sciences (ICCIS), 2011 International Conference on*. 2011.
[6] Tanimoto S., Hiramoto M., Iwashita M., Sato H., et al., Risk management on the security problem in cloud computing. In *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on*. 2011.
[7] Szefer J., Jamkhedkar P., Chen Y. & Lee R., Physical attack protection with human-secure virtualization in data centers. In *Dependable Systems and Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference on*. 2012.
[8] ITU-T Study Group VII, ITU-T Rec. X.800 (03/91) Security architecture for Open Systems Interconnection for CCITT applications, **International Telecommunication Union**, 1991. *http://www.itu.int/rec/T-REC-X.800-199103-I/en*
[9] ITU-T Study Group 17, ITU-T Rec. X.805 (10/2003) Security architecture for systems providing end-to-end communications, **International Telecommunication Union**, 2003. *http://www.itu.int/rec/T-REC-X.805-200310-I/en*
[10] Mell P. & Grance T., The NIST Definition of Cloud Computing, **National Institute of Standards and Technology**, 2011. *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*
[11] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing Version 2.1, (2009, Desember). *http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf*
[12] Nurmi D., Wolski R., Grzegorczyk C., Obertelli G., et al., The eucalyptus open-source cloud-computing system. In *Cluster Computing and the Grid (CCGRID). 9th IEEE/ACM International Symposium on*. 2009.
[13] Eucalyptus Systems Inc., Eucalyptus Installation Guide, (2013, Maret). *http://www.eucalyptus.com/docs/3.2/ig/*
[14] The Hacker's Choice, THC-SSL-DOS: a tool to verify the performance of SSL, (2011, Oktober). *http://www.thc.org/thc-ssl-dos*
[15] Bernat, Vincent, SSL computational DoS mitigation, (2011, Nopember). *http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html*
[16] Lyman Ott R. & Longnecker M., An introduction to statistical methods and data analysis, sixth edition. Brooks/Cole, Cengage Learning, 2010.