Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Analisis Sistem Keamanan Pada *Cloud Computing* Menggunakan Metode *Attack-Centric* (*Security System Analysis of Cloud Computing Using Attack-Centric Method*)

Aditya Dwi P.W. [1*], E.I.H. Ujianto [2]
[1,2] Program Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
[1,2] Jl. Ring Road Utara Daerah Istimewa Yogyakarta
[2]erik.iman@uty.ac.id
**Corresponding Author*: adityadwi.putrowicaksono@student.uty.ac.id

Abstrak

Seiring dengan makin pesatnya perkembangan teknologi penyimpanan data, *Cloud Computing* merupakan salah satu dari beberapa teknologi jaringan penyimpan data yang sedang berkembang pesat saat ini. Tidak menutup kemungkinan data yang tersimpan dalam cloud computing merupakan data penting dan rahasia yang tidak semua orang bisa mengaksesnya. hal ini menyebabkan keamanan data merupakan suatu hal yang sangat penting, Banyak ahli dan praktisi berpendapat bahwa *Enterprise Computing* adalah suatu masalah yang sudah selesai, cenderung stabil dan statis, serta tidak membutuhkan suatu peningkatan yang signifikan. dibalik kelebihan yang ada pada teknologi *Cloud Computing* juga ada beberapa ancaman, salah satunya keamanan data yang ada pada sistemasi *Cloud Computing*. Ancaman ini bisa diartikan seperti kebocoran data penting/rahasia, pencurian *credential*, peretasan API, pembajakan *account*, dan kehilangan data secara permanen maupun penyalahgunaan layanan *cloud*. Untukmenjaga agar data aman dari pengguna yang tidak berhak maka diperlukan Analisis sistem keamanan pada media penyimpanan *Cloud Computing*. Dalam tulisan ini akan dibahas tentang analisis dan standar sistem keamanan pada *Cloud Computing*, yang mana penulis juga akan memberikan rekomendasi dan alasan terkait teknik keamanan yang paling tepat untuk diaplikasikan ke dalam arsitektur *Cloud Computer* dan menentukan standar keamanan pada *Cloud Computing*.

Kata Kunci: *Sistem Keamanan, Cloud Computing, Enterprise Computing*

Abstract

Along with the rapid development of data storage technology, Cloud Computing is one of several data storage network technologies that is currently growing rapidly. Did not rule out the data stored in cloud computing is important and confidential data that is not accessible to everyone. This causes data security is very important. Many experts and practitioners argue that Enterprise Computing is a problem that has already been resolved, tends to be stable and static, and does not require a significant increase. behind the advantages that exist in cloud computing technology there are also several threat, one of them is data security in cloud computing. this threat can be interpreted as leakage of important / confidential data, credential theft, API hacking, account hijacking, and permanent data loss or misuse of cloud services. to keep data safe from unauthorized users, it is necessary to analyze the security system on Cloud Computing storage media. in this paper we will discuss the analysis and security system standards in Cloud Computing, which the author will also provide recommendations and reasons related to the most appropriate security techniques to be applied to the cloud computer architecture and determine security standards in cloud computing.

Keywords*: System Security, Cloud Computing, Enterprise Computing*

1. Pendahuluan

Diera perkembangan teknologi saat ini *Cloud Computing* merupakan teknologi yang memiliki banyak kelebihan. Karena model komputasi ini memungkinkan *user* untuk menggunakan *resource* misalnya *network, server, storage, application* dan *service* yang ada dalam sebuah sistem jaringan *cloud*, disisi lain juga dapat di share sekaligus digunakan secara bersama. Selain itu *cloud computing* juga memiliki kelebihan yakni dapat meningkatkan fleksbilitas dan kapabilitas dari proses computer 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 yang dikatakan oleh John D. Howard, seorang *Analisys of Security Incidents on the Internet* pada tahun 1989-1995, mengatakan bahwa: "*Computer Security is preventing attacker form achieving objectives through unauthorized access or unauthorized use of computer and network*". Yakni proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara illegal dari komputer dan jaringan [1].

Beberapa ancaman di dalam jaringan komputer meliputi ancaman fisik berupa pencurian perangkat keras, kerusakan pada komputer dan perangkat komunikasi jaringan, *wiretapping*dan bencana alam. Ancaman yang bersifat logik berupa kerusakan pada sistem operasi atau aplikasi, virus, dan *sniffing*. Ancaman lain berupa *sniffer* (peralatan yang memonitor proses yang sedang berlangsung), *spoofing* (penggunaan komputer untuk meniru, dengan cara menimpa identitas MAC *Address* atau alamat IP), Phreaking (perilaku menjadikan sistem pengamanan telepon melemah), *remote attack, hole* (kondisi dari *software* dan hardware yang bisa diakses oleh pemakai yang tidak memiliki otoritas), *hacker dan cracker*.

Pada tahun 2013 AKAMI melaporkan Indonesia menjadi nomor 1 sebagai sumber serangan internet (*malicious traffic*). Trafik serangan dari IP Indonesia berkisar 38% dari seluruh serangan di internet dibandingkan trafik dari sekitar 175 negara yang diteliti. Trafik serangan ini meningkat hampir 2 kali lipat dibandingkan dengan data sebelumnya yaitu sekitar 21%. AKAMAI dalam laporan tersebut menyatakan bahwa IP yang terdeteksi sebagai sumber serangan bisa jadi tidak mencerminkan lokasi penyerang. Karena bisa saja seorang penyerang dari Amerika Serikat, Cina ataupun negara lainnya melancarkan serangan dari IP Indonesia melalui jaringan botnet atau computer yang terinfeksi malware di ASEAN cukup tinggi, yakni sebesar 16,88%. Dari laporan tersebut, malware yang banyak beredar di Indonesia di antaranya adalah Ramnit dan Sality. Sedangkan berdasarkan hasil survey *malware* yang dilakukan ID-CERT, 52% malware yang dilaporkan adalah Adware dan 35%-nya adalah Trojan, sisanya merupakan Virus, *Worm, Keylogger, Spyware* dan *Backdoor*. Seiring dengan semakin berkembangnya *cloud computing*, peningkatan performa dalam soal sistem keamanan dan ketersediaan jaringan menjadi hal yang sangat penting. Hal ini dikarenakan *cloud computing* sangat berkaitan dengan pengaksesan aplikasi perangkat lunak dan penyimpanan data *private* atau *public* secara *online*, sehingga harus tersedia kapanpun dan dimanapun saat dibutuhkan.

Paper ini membahas tentang analisis dan standar sistem keamanan pada *Cloud Computing*, yang mana penulis juga akan memberikan rekomendasi dan alasan terkait teknik keamanan yang paling tepat untuk diaplikasikan ke dalam arsitektur *cloud computer* sekaligus menjelaskan standar keamanan pada *cloud computing*. Dalam menganalisis berbagai serangan yang ada dan untuk mengklasifikasikan model teknik keamanan yang sudah di impementasikan ataupun yang belum di implementasikan penulis akan menerapkan metode *Attack-Centric*. Dengan adanya tulisan ini diharapkan bisa mengurangi/meminimalisir ancaman dari perspektif manapun dalam hal penerapan teknologi *cloud computing*.

2. Tinjauan Pustaka

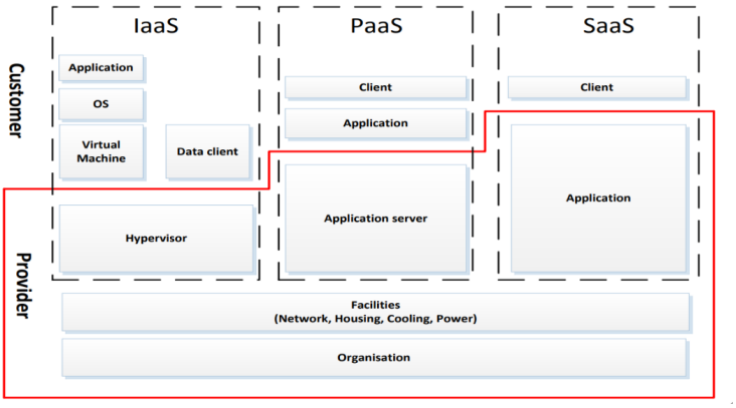
Cloud computing menurut *National Institute of Standards and Technology* (NIST) adalah suatu model komputasi yang memberikan kemudahan, kenyamanan, dan sesuai dengan permintaan (*on-demand access*) untuk mengakses dan mengonfigurasi sumber daya komputasi (*network, servers, storage, applications, and service*) yang bisa dengan cepat dirilis tanpa adanya banyak interaksi dengan penyedia layanan [2].

Jenis layanan cloud *computing* dibedakan menjadi tiga yakni, *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) dan *Software as a Service* (SaaS).

Infrastructure as a Service (IaaS): IaaS menyediakan penyimpanan atau sumber daya komputasi yang dapat diakses *online*. Misalnya, *Google Cloud Storage, Microsoft Windows Azure Storage*, dan *Dropbox*.

Platform as a Service (PaaS): PaaS menyediakan sebuah platform kepada pelanggan untuk menjalankan aplikasi. Biasanya PaaS menyediakan *software development tool* untuk membangun suatu aplikasi pada platform. Jenis aplikasi umum yang biasa dijalankan pada platform adalah suatu skrip (seperti PHP, Python) atau kode *byte* (seperti C#). Contoh penyedia PaaS, seperti Google App Engine atau Microsoft Azure.

Software as a Service (SaaS): SaaS menyediakan akses penuh terhadap *software* atau aplikasi. Aplikasi tersebut seperti email server, email client, atau document editor. Biasanya layanan SaaS dapat diakses melalui browser. Ilustrasi jenis-jenis layanan cloud adalah seperti pada gambar 1.



Gambar 1. Mengilustrasikan Layanan *Cloud*

Kelebihan dari *cloud computing* ini juga diimbangi dengan adanya beberapa kelemahan, terutama dalam segi keamanan penyimpanan data. Dasar dari cloud computing yang *share resource* mengakibatkan keamanan data terutama yang bersifat private rawan dibobol. Sugiyanto [3] dan Andrew et al [4] 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). Ida Bagus et al. [5] 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.

Disebutkan oleh George Reese, bahwa dalam praktiknya *user cloud computing* memiliki risiko yang mungkin dihadapi sebagai berikut:

1) Provider penyedia jasa *cloud computing* mengalami kebangkrutan sehingga server berhenti bekerja dan data hilang lalu tidak dapat dipertanggungjawabkan *provider.*
2) Pihak lain (yang tidak ada hubungannya dengan user) melakukan penggugatan pada *provider* jasa layanan cloud, yang kemudian memiliki hak akses kepada seluruh *server cloud* dan mengancam kerahasiaan data user.
3) Kegagalan pihak penyedia layanan *cloud* dalam melakukan perawatan infrastruktur dan fisik akses kontrol.

3. Metodologi

Paper ini menganalisa teknik-teknik yang memang telah digunakan maupun teknik teknik yang masih dalam proses pengembangan, selain itu juga akan ditentukan teknik keamanan yang paling tepat untuk diaplikasikan ke dalam arsitektur *cloud computer* dan menentukan standar keamanan pada *cloud computing*.

Metode yang diterapkan untuk melakukan pengkajian adalah metode *Attack-Centric*. Metode ini dilakukan dengan tiga langkah berikut:

1) Menganalisa apakah tujuan dari serangan tersebut (contoh: untuk menganalisis jenis trafik dengan menangkap dan menganalisis paket-paket data yang ada pada trafik tersebut).

2) Menganalisa bagaimana sebuah serangan dapat terjadi (contoh: menentukan titik di mana seorang penyerang harus mengawasi paket-paket yang melintas).
3) 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.

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.

Di dalam penelitian ini, akan ada 4 serangan keamanan yang akan diteliti, di mana serangan tersebut akan menyebabkan kebocoran dan kehilangan data, Serangan-serangan keamanan tersebut diantaranya:

1. *Snooping Attack*

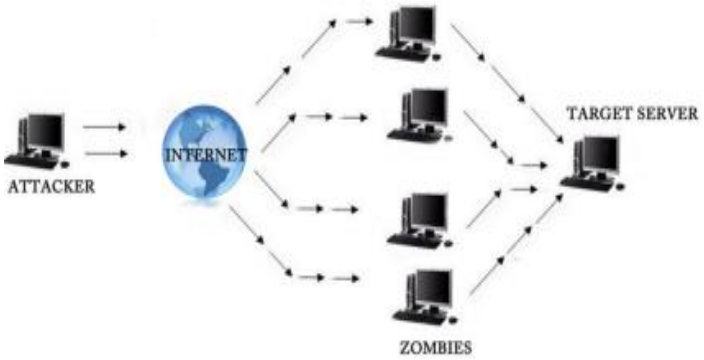
Snooping attack adalah kondisi dimana seorang penyerang akan melihat paket data yang mengalir di dalam jaringan. Snooping attack bersifat pasif, penyerang tidak akan memodifikasi paket data yang telah dia lihat [6]. Seorang penyerang akan mengambil konten-konten yang tersimpan pada komputer user, sehingga 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*

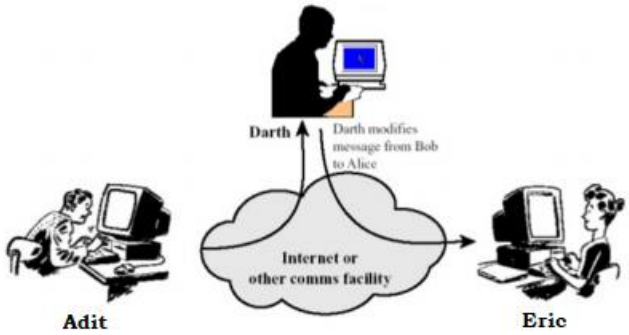
DoS *attack* adalah serangan yang bertujuan untuk membuat sebuah *server* atau website tidak dapat diakses oleh user lain. Salah satu contoh serangan yang dapat dilakukan adalah dengan membanjiri jaringan dengan paket-paket sampah [7]. Dengan menerapakan serangan ini, *server* penyedia *cloud* akan menjadi *down*, sehingga dapat dengan mudah dimasuki oleh seorang penyerang.



Gambar 2. Mengilustrasikan 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* [8]. 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.



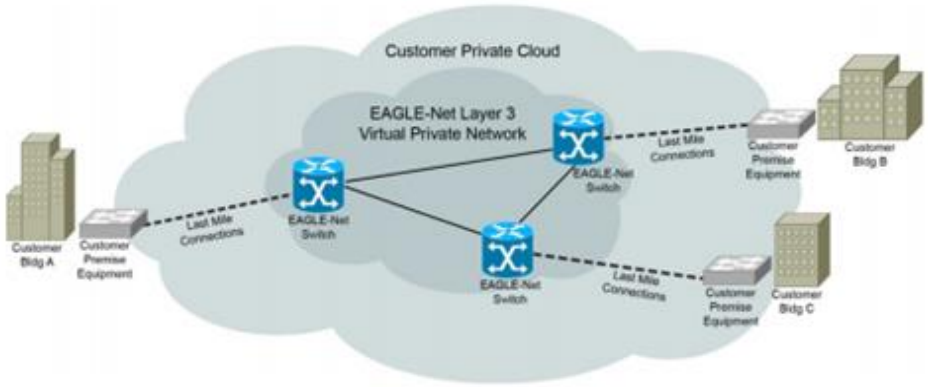
Gambar 3. Mengilustrasikan *Man-in-The-Middle Attack*.

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.

Beberapa konsep (*Current Cloud Computing Network*) sistem keamanan jaringan yang diterapkan pada cloud computing saat ini adalah:

a. 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.



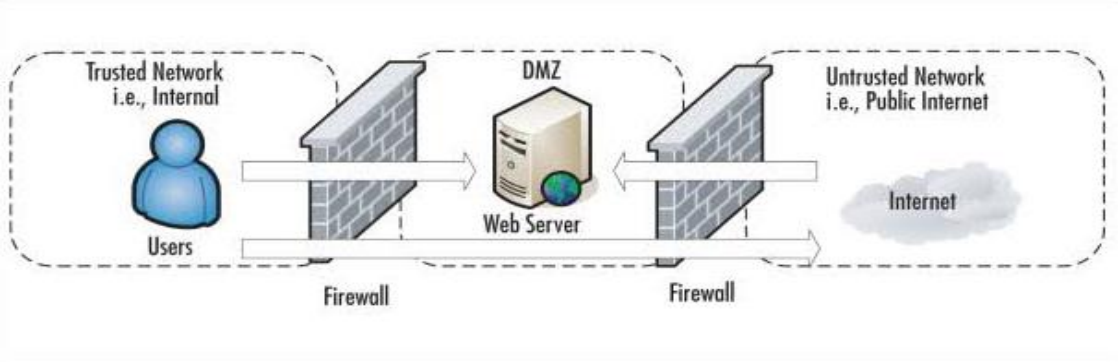
Gambar 4. Mengilustrasikan VPN pada jaringan cloud

b. 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 [9].

c. *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*.



Gambar 5 Mengilustrasikan *Firewall* pada Jaringan *Cloud*

Dari ketiga konsep sistem keamanan pada cloud computing diatas, ada juga beberapa sistem keamanan masa depan (*Future Cloud Computing*) yang sangat memungkinkan untuk di Implementasikan pada cloud computing, Sistem ini sering disebut NEBULA.

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 [10], diantaranya:

a. *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 keamanan, maka onion routing dapat diimplementasikan pada NEBULA.

b. *Proof of Path (PoP)*

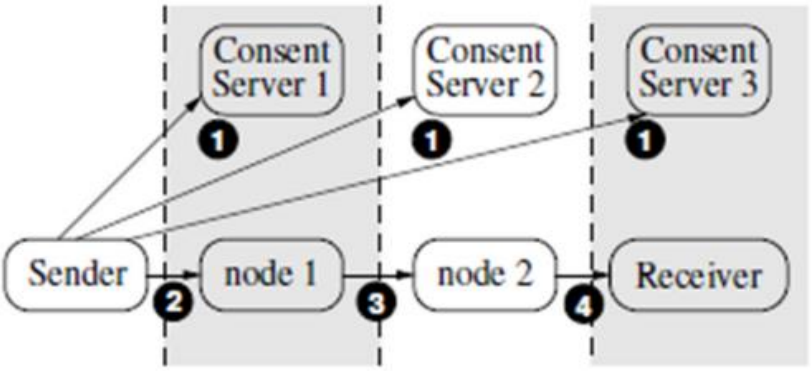
PoP adalah mekanisme yang bertujuan untuk memastikan bahwa jalur yang akan dilalui oleh paket data telah diautentikasi. Dengan demikian, paket-paket akan melewati jalur yang legal sehingga akan mencegah terjadinya banjirnya paket pada jaringan NEBULA, atau disebut *packet flooding* [8].

c. *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, tidakada *user* ilegal yang berada di dalam NEBULA, sehingga walau pun ada serangan dari dalam NEBULA maka akan lebih cepat terdeteksi dan diatasi [11].

d. 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 [12].



Gambar 6. Mengilustrasikan skema teknik ICING

4. Hasil dan Pembahasan

Dalam konsep sistem keamanan jaringan *cloud computing* saat ini (*Current Cloud Computing Network*) terhadap beberapa serangan keamanan diatas adalah sebagai berikut:

Tabel 1. Kapabilitas (*Current Cloud Computing Network*)

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.

Dan dalam konsep sistem keamanan jaringan *cloud computing* di masa depan atau sering disebut juga dengan NEBULA (*Future Cloud Computing*) terhadap beberapa serangan keamanan diatas adalah sebagai berikut:

Tabel 2. Kapabilitas (*Future Cloud Computing*)

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 (*Future Cloud Computing*) 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*.

Cloud Computing merupakan suatu model yang memberikan kenyamanan akses suatu jaringan sesuai keperluan pada suatu wadah bersama terdiri atas sumber daya komputasi (seperti jaringan, *server,* penyimpanan, aplikasi, dan layanan) yang dapat dikonfigurasi dengan cepat [13]. Namun, dibalik kenyamanan tersebut terdapat beberapa ancaman yang dapat membahayakan, baik individu, kelompok, bahkan negara. Beberapa ancaman yang dapat membahayakan cloud computing adalah kebocoran data, pencurian kredensial, peretasan API, eksploitasi kerentanan sistem, pembajakan akun, hilangnya data secara permanen, penyalahgunaan layanan *cloud*, dan serangan DOS [14]. Oleh karena itu, perlu ada standar keamanan yang diterapkan pada penyedia *cloud computing*. Selain itu, perlu juga hukum yang membatasi penggunaan cloud computing, terutama data yang menyangkut banyak orang dan data rahasia.

Suatu penyedia *cloud computing* perlu memenuhi standard untuk menjamin keamanan penggunanya. Berikut ini merupakan pemetaan standard keamanan yang perlu diperhatikan oleh penyedia cloud computing [15].

1. Standar Ketersediaan

Tabel 3. Standard keamanan: ketersediaan (*availability*)

Kategori	Standard yang Tersedia	Organisasi
Ketersediaan	ATIS-02000009	ATIS
	Cloud Services Lifecycle Checklist	
	ISO/PAS 22399:2007	ISO
	Societal security – Guideline for incident preparedness and operational continuity management	

2. Standar Autentikasi dan Otorisasi

Tabel 4. Standard keamanan: autentikasi dan otorisasi

Kategori	Standard yang Tersedia	Organisasi
Autentikasi dan Otorisasi	RFC 5246	IETF
	Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	
	RFC 3820: X.509	IETF
	Public Key Infrastructure (PKI) Proxy Certificate Profile	
	RFC5280: Internet X.509	IETF
	Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
	RFC 5849	IETF
	OAuth (Open Authorization Protocol)	
	ISO/IEC 9594-8:2008 | X.509	ISO/IEC
	Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks	& ITU-T
	ISO/IEC 29115 | X.1254	ISO/IEC
	Information technology — Security techniques — Entity authentication assurance framework	& ITU-T
	FIPS 181	NIST
	Automated Password Generator	
	FIPS 190	NIST
	Guideline for the Use of Advanced Authentication Technology Alternatives	
	FIPS 196	NIST
	Entity Authentication Using Public Key Cryptography	
	OpenID Authentication	OpenID
	eXtensible Access Control Markup Language (XACML)	OASIS
	Security Assertion Markup Language (SAML)	OASIS

3. Standar Kerahasiaan

Tabel 5. Standard keamanan: kerahasiaan (*confidentiality)*

Kategori	Standard yang Tersedia	Organisasi
Kerahasiaan	RFC 5246	IETF
	Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	
	Key Management Interoperability Protocol (KMIP)	OASIS
	XML Encryption Syntax and Processing	W3C
	FIPS 140-2	NIST
	Security Requirements for Cryptographic Modules	
	FIPS 185	NIST
	Escrowed Encryption Standard (EES)	
	FIPS 197	NIST
	Advanced Encryption Standard (AES)	
	FIPS 188	NIST
	Standard Security Label for Information Transfer	

4. Standar Integritas

Tabel 6. Standard keamanan: integritas (*integrity)*

Kategori	Standard yang Tersedia	Organisasi
Integritas	XML signature (XMLDSig)	W3C
	FIPS 180-4	NIST
	Secure Hash Standard (SHS)	
	FIPS 186-4	NIST
	Digital Signature Standard (DSS)	
	FIPS 198-1	NIST
	The Keyed-Hash Message Authentication Code (HMAC)	

5. Standar Manajemen Identitas

Tabel 7. Standard keamanan: manajemen identitas

Kategori	Standard yang Tersedia	Organisasi
Manajemen identitas	X.idmcc	ITU-T
	Requirement of IdM in Cloud Computing	
	FIPS 201-1	NIST
	Personal Identity Verification (PIV) of Federal Employees and Contractors	
	Service Provisioning Markup Language (SPML)	OASIS
	Web Services Federation Language (WS-Federation) Version 1.2	OASIS
	WS-Trust 1.3	OASIS
	Security Assertion Markup Language (SAML)	OASIS
	OpenID Authentication 1.1	OpenID Foundation

6. Standar Monitor Keamanan dan Respon Insiden

Tabel 8. Standard keamanan: monitoring keamanan dan respon insiden

Kategori	Standard yang Tersedia	Organisasi
Monitoring Keamanan dan Respon Insiden	ISO/IEC WD 27035-1	ISO/IEC
	Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management	
	ISO/IEC WD 27035-3	ISO/IEC
	Information technology — Security techniques — Information security incident management — Part 3: Guidelines for CSIRT operations	
	ISO/IEC WD 27039; Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems	ISO/IEC
	ISO/IEC 18180	ISO/IEC
	Information technology – Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2 (NIST IR 7275)	
	X.1500	ITU-T
	Cybersecurity information exchange techniques	
	X.1520: Common vulnerabilities and exposures	ITU-T
	X.1521	ITU-T
	Common Vulnerability Scoring System	
	PCI Data Security Standard	PCI
	FIPS 191	NIST
	Guideline for the Analysis of Local Area Network Security	

7. Standar Kendali Keamanan

Tabel 9. Standard keamanan: kendali keamanan

Kategori	Standard yang Tersedia	Organisasi
Kendali Keamanan	Cloud Controls Matrix Version 1.3	CSA
	ISO/IEC 27001:2005	ISO/IEC
	Information Technology – Security Techniques Information Security Management Systems Requirements	
	ISO/IEC WD TS 27017	ISO/IEC
	Information technology — Security techniques — Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	
	ISO/IEC 27018	ISO/IEC
	Code of Practice for Data Protection Controls for Public Cloud Computing Services	
	ISO/IEC 1st WD 27036-4	ISO/IEC
	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services	

8. Standar Manajemen Kebijakan Keamanan

Tabel 10. Standard keamanan: manajemen kebijakan keamanan

Kategori	Standard yang Tersedia	Organisasi
Manajemen Kebijakan Keamanan	ATIS-02000008	ATIS
	Trusted Information Exchange (TIE)	
	FIPS 199	NIST
	Standards for Security Categorization of Federal Information and Information Systems	
	FIPS 200	NIST
	Minimum Security Requirements for Federal Information and Information Systems	
	ISO/IEC 27002	ISO/IEC
	Code of practice for information security management	
	eXtensible Access Control Markup Language (XACML)	OASIS

Berdasarkan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) [16] dan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) [16], penyedia layanan cloud computing termasuk ke dalam kategori Penyelenggara Sistem Elektronik (PSE) yang perlu mematuhi aturan-aturan berikut [17].

1. Kewajiban pendaftaran bagi PSE pelayanan publik (Pasal 5)
2. Kewajiban sertifikasi kelaikan hardware (Pasal 6)
3. Kewajiban didaftarkannya software bagi PSE pelayanan publik (Pasal 7)
4. Ketentuan tentang penggunaan tenaga ahli (Pasal 10)
5. Kewajiban-kewajiban dalam tata kelola sistem elektronik (Pasal 12)
6. Penerapan manajemen risiko penyelenggaraan sistem elektronik (Pasal 13)
7. Kewajiban memiliki kebijakan tata kelola dan SOP (Pasal 14)
8. Kewajiban dan ketentuan tentang pengelolaan kerahasiaan, keutuhan, dan ketersediaan data pribadi (Pasal 15)
9. Pemenuhan persyaratan tata kelola bagi PSE untuk pelayanan publik (Pasal 16)
10. Penempatan pusat data dan pusat pemulihan bencana serta mitigasi atas rencana keberlangsungan kegiatan penyelenggara sistem elektronik (Pasal 17)
11. Pengamanan penyelenggaraan sistem elektronik (Pasal 18 s.d. 19)
12. Kewajiban sertifikasi kelaikan sistem bagi PSE pelayanan publik (Pasal 30 s.d. 32)

5. Kesimpulan

Dari hasil pembahasan yang telah dilakukan, maka dapat disimpulkan bahwa:

1) Konsep sistem keamanan yang telah terimplementasikan saat ini (*Current Cloud Computing Network*) belum cukup untuk mengatasi seluruh serangan keamanan yang telah diteliti, hal ini dikarenakan tidak fleksibelnya jaringan *cloud computing* untuk mengaplikasikan mekanisme keamanan.
2) Konsep sistem keamanan pada NEBULA (*Future Cloud Computing*) diantaranya: PoC, PoP, dan ICING jauh lebih baik dalam hal mengatasi beberapa serangan yang telah diteliti, yakni *Snooping attack*, *DoS attack* dan *man-in-the-niddle attack*. Konsep sistem keamanan ini sangat memungkinkan menggunakan pemakaian *onion routing* yang dapat diimplementasikan dengan cepat pada nebula untuk mengatasi serangan *Traffic analysis.*
3) Dibalik kelebihan teknologi *cloud computing*, privacy data merupakan hal penting dalam sebuah organisasi terutama pengguna *Cloud Computing* yang harus memperhatikan aspek proteksi data yang disediakan oleh provider. tidak menutup kemungkinan data yang tersimpan dalam *cloud computing* merupakan data penting dan rahasia yang tidak semua orang bisa mengaksesnya. Jika *provider* mengalami *down*, data organisasi terancam hilang, tidak dapat diakses, atau dapat *direcovery* namun tidak utuh, Hal tersebut tentu saja dapat merugikan pihak user. Dari hasil pembahasan, penulis menyimpulkan bahwa user sangat perlu bersifat selektif untuk memilih atau menentukan *provider* penyedia layanan *Cloud Computing*. Langkah terbaik yakni menentukan *Provider* penyedia Layanan sesuai pemetaan standard keamanan yang perlu diperhatikan oleh penyedia *cloud computing*.

DAFTAR REFERENSI

[1] Dewannata D. Tujuan, Risiko dan Ancaman pada Keamanan Jaringan Komputer. www.ilmukomputer.com. Tanggal akses terakhir: 28 Juli 2016.

[2] Mell, P., Grance, T. *The NIST Definition of Cloud computing Recommendations of the National Institute of Standards and Technology*, NIST Spec. Publ. 2011: 80-145.

[3] Sugiyanto. Prototipe Sistem Informasi Haji Untuk Menangani Jemaah Tersesat Menggunakan SMS Gateway. Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI). 2014; 3(2): 123-128.

[4] Osmond, A. B., Nugroho, L. E., & Kusumawardhani, S. S. Aplikasi Pengumpulan Data Survei Memanfaatkan SMS Gateway. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*. 2016; *5*(1): 1-5.

[5] Manuaba, I. B. V. H., Hidayat, R., & Kusumawardani, S. S. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada). *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*. 2012; *1*(1): 13-17.

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

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

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

[9] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*. 2012; *1*(1), 11.

[10] 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. 2013; 7858: 1–24

[11] 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. 2011: 1–31.

[12] Naous, J., Walfish, M., Nicolosi, A., Mazières, D., Miller, M., & Seehra, A. (2011, December). Verifying and enforcing network paths with ICING. In *Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies.* 2011: 1-12.

[13] Mell, P., Grance, T. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology, Nist Spec. 2011; 145: 7.

[14] Rashid, F.Y. The dirty dozen: 12 cloud security threats, 2016. [Online]. Available: https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

[15] Bumpus, W. NIST Cloud Computing Standards Roadmap, NIST Cloud Comput. Stand. 2013: 1-3.

[16] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi danTransaksi Layanan Elektronik. 2008; 1: 1–29.

[17] *Government of Indonesia*. PP No. 82/2012 Penyelenggaraan Sistem dan Transaksi Elektronik. 2012: 1–54.