BAB I
PENDAHULUAN

1.1 Latar Belakang

Paradigma *cloud computing* memiliki karakteristik yang telah dibayangkan sejak kurang lebih 60 tahun yang lalu. *Cloud computing* menawarkan komputasi yang terukur atau elastis pada alat komputasi yang lengkap secara virtual, mendukung semua tekno*log*i *software* dan *tools*, dan melayani melalui jaringan yang berbeda sehingga *cloud computing* menjadi *platform* yang independen, *portable*, dan dapat diakses dimana-mana. *Cloud computing* juga memiliki kemampuan untuk memberi pelayanan yang sesuai dengan permintaan, pembagian, pengambilan, dan pelepasan sumber daya komputasi yang bisa dikonfigurasi secara instan membuat *cloud computing*, elastis, berkelanjutan, dan medekati komputasi utilitas (Mell dan Grance ,2011).

Cloud computing sepertinya membawa komputasi kepada kehidupan orang-orang biasa yang memiliki desktop virtual di *cloud*. Dan saat dunia yang haus akan sumber daya menghadapi masa sulit untuk menyerahkan sumber daya nya pada kebutuhan komputasi yang sedang berkembang seperti konsep *smart city* dan pengoprasian nya dan evolusi dari *big data*. *Cloud computing* dapat menjadi jawaban untuk berbagai macam tantangan yang ada di dunia. Kemungkinan satu-satunya penghalang atau rintangan untuk *cloud computing* saat ini adalah ancaman keamanan atau kesulitan dalam mencapai kode yang telah bersih dari *bug* dan celah keamanan (Ahmad, 2017).

Seiring dengan berjalannya waktu, *cloud computing* menggabungkan banyak teknologi-teknologi baru dan canggih yang mengakibatkan sistem dan jaringan menjadi rumit, karena itu kemunculan masalah mungkin terjadi. Setiap lapisan mungkin mengalami kerentanan tertentu, dikarenakan oleh kesalahan pemrograman atau konfigurasi yang berbeda dari pengguna atau penyedia. Sebagai contoh, sebuah aplikasi *online shop* yang dijalankan menggunakan *Google App Engine*. Terdiri dari beberapa halaman produk, area *login*, dan fungsi sederhana untuk memberi komentar dan ulasan terhadap sebuah produk. Setelah

masuk ke halaman web dan memberikan kredensial yang valid, pengguna mendapatkan *cookie session* untuk mengidentifikasi dirinya dalam sesi tersebut. Fungsi komentar dari toko web rentan terhadap serangan *CrossSite-Scripting* (XSS). Pada kasus aplikasi web, serangan XSS adalah serangan yang biasa terjadi. Menurut Gupta (2016) celah yang disebabkan oleh XSS ada pada hampir 80% layanan *Online Social Networking* (OSN) yang berbasis *cloud*. Selain XSS serangan SQL (Structured Query Language) atau yang biasa disebut SQL injection attack dapat mengancam layanan *cloud computing* khususnya pada sisi pengguna. Pada tahun 2008 sampai 2010 terjadi pembobolan secara besar-besaran terhadap layanan web yang disebabkan oleh botnet ASPROX yang menyebabkan infeksi pada website dalam waktu singkat. ASPROX menggunakan SQL queries khusus untuk menysupi database website. ASPROX biasanya menysupkan link iframe kedalam database, yang menyebabkan pengguna website yang terinfeksi teralihkan laman nya kepada website jahat yang digunakan untuk menyebarkan malware kepada sistem pengguna.

Secara umum penyerang dapat menyebrang lapisan infrastruktur berbeda pada arsitektur *cloud* menggunakan serangan khusus pada implementasi infrastruktur. Infrastruktur *cloud computing* yang terkompromi dapat digunakan untuk melancarkan serangan *Distributed Denial of Service* (DDoS) pada jaringan yang besar. Serangan berjenis DDoS sendiri sudah menjadi ancaman yang tidak jarang bagi bisnis berbasis online. Terdapat sekitar lebih dari lima puluh ribu serangan berjenis DDoS saja perminggunya secara global (Srivastava, 2011).

Menurut Roschke, (2009) *Intrusion Detection System* (IDS) dapat menjadi solusi terhadap kejahatan pada sistem elektronik khususnya pada *cloud computing*. Ini dikarenakan fungsi IDS yang memonitor lalu lintas jaringan sehingga dapat mencegah serangan seperti DDOS, *scanning attack, penetration attack,* dan lain-lain.

IDS merupakan alat keamanan lainnya seperti *software antivirus, firewalls* dan *access controll scheme,* yang digunakan untuk memperkuat keamanan dari informasi dan komunikasi sistem (Gracia-Teodoro, 2009). Secara umum IDS terbagi menjadi dua macam, *anomaly detection* dan *signature detection. Anomaly detection* memeriksa aktivitas jahat melalui pola tingkah laku dari lalu lintas

jaringan. Sedangkan *signature detection* mendeteksi keanehan melalui paket atau *logs* yang sebelumnya telah didefinisikan sebagai tanda-tanda serangan (Dildar, 2017).

Salah satu kelemahan dari IDS berbasis *signature* adalah, ketidak mampuan IDS mendeteksi serangan baru. Menurut Gronland (2006), IDS berbasis *signature* masih banyak dipergunakan, dan jika terdapat serangan baru, IDS tersebut tidak dapat mengetahuinya, salah satu cara mengatasi masalah ini adalah dengan membuat peraturan atau *rules* baru setiap serangan baru muncul dengan menggunakan *honeypot*. *Honeypot* itu sendiri adalah sebuah sistem atau *tools* untuk menjebak penyerang atau penyusup, agar metode atau prilaku penyerang dapat diselidiki. Dengan menggunakan *honeypot* kita bisa yakin bahwa semua lalu lintas yang menujunya dianggap jahat. Ini dikarenakan *honeypot* sendiri tidak memiliki aktivitas produksi dan tidak memiliki aktivitas yang berotoritas. Sehingga dapat dipastikan bahwa setiap aktivitas didalam *honeypot* merupakan aktivitas jahat, hal tersebut dapat dimanfaatkan IDS untuk membuat *rules* baru terhadap serangan yang baru, dengan cara merubah *log* serangan baru di *honeypot* menjadi *rules* baru untuk IDS.

Dikarenakan sifat *cloud* yang memiliki banyak *Virtual Machine* (VM), maka IDS yang ada pun harus mengimbangi jumlah VM tersebut dan dikarenakan sifat IDS yang tidak bisa mendeteksi serangan baru, maka dibutuhkan sebuah mekanisme atau cara untuk memperbaharui *rules* dari IDS disetiap VM yang ada.

Pada penelitian ini mekanisme pembaharuan *rules* IDS dilakukan dengan proses pendistribusian *rules*. Pertama *rules* dibuat oleh sebuah VM atau mesin komputer. Pembuatan *rules* dilakukan dengan menggunakan *log honeypot* seperti yang telah dibahas. Kemudian *rules* tersebut dibagikan kepada VM lain yang berada di *cloud computing*. Pada penelitian ini proses distribusi dibantu menggunakan dua algoritma utama yaitu RSA (*Rivest-Shamir-Adleman*) sebagai *digital signature* untuk verifikasi *rules* dan BFS (*Breadth First Search*) untuk mempercepat proses pembagian *rules*. Untuk memasitikan VM yang berada di *cloud* mendapatkan *rules* yang benar dan asli dari pembuat *rules*, dibutuhkan sebuah mekanisme keamanan. Pada penelitian ini pengamanan dilakukan dengan menggunakan *digital signature*. *Digital signature* digunakan karena memiliki

aspek *authentification*. Dikarenakan aspek tersebut, penerima *rules* dapat melakukan pemeriksaan keaslian *rules* yang diterima.

Penggunaan algoritma RSA sebagai *digital signature*, tentunya dapat menurunkan performa VM sehingga waktu yang diperlukan untuk melakukan pekerjaan setiap VM akan bertambah. Berdasarkan penelitian Preetha(2013) untuk melakukan proses enkripsi dan dekripsi menggunakan algoritma RSA terhadap file berukuran 14kb membuthkan waktu 62 detik. Oleh karena itu penelitian ini menggunakan algoritma BFS untuk menutupi penambahan waktu yang disebabkan oleh algoritma RSA. Pada penelitian ini BFS digunakan untuk mencari jalur tercepat saat porses distribusi file *rules*.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut dapat dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana cara melakukan verifikasi *rules* menggunakan *digital signature* RSA?
2. Bagaimana Mengantisipasi turunnya performa dikarenakan adanya protokol keamanan tambahan?

1.3 Tujuan Penelitian

Setelah diketahui rumusan masalahnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Memverifikasi *rules* dengan menggunakan *digital signature* RSA
2. Mengantisipasi turunnya performa dikarenakan adanya protokol keamanan tambahan.

1.4 Manfaat Penelitian

Adapun penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Mempercepat pendistribusian *rules* pada VM di *cloud computing*.
2. Memberikan pengetahuan tentang pembuatan *rules* dari *log honeypot*.
3. Mengantisipasi turunnya performa dikarenakan adanya protokol keamanan tambahan

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini difokuskan kepada distribusi *rules* IDS dengan bantuan algoritma BFS dan RSA.

2. Uji coba penelitian ini difokuskan terhadap *rules* IDS.

1.6 Sistematika Penulisan

Penelitian ini menggunakan struktur penulisan dengan rincian sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang diadakannya penelitian, yang disusun berdasarkan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II KAJIAN PUSTAKA

Bab ini menjelaskan teori-teori yang terlibat di dalam penelitian yang meliputi *cloud computing*, kriptografi, fungsi hash, *digital signature*, algoritma RSA serta BFS.

BAB III METODO*LOG*I PENELITIAN

Bab ini menjelaskan langkah-langkah yang akan dilaksanakan serta alat-alat yang akan digunakan di dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi penjelasan dan materi yang memiliki keterkaitan dengan tujuan penelitian serta jawaban dari pertanyaan yang menjadi dasar penelitian ini. Isi dari bagian adalah penjelasan tentang aplikasi yang telah dibuat, detail data penelitian yang digunakan, desain dan hasil eksperimen beserta analisisnya, serta evaluasi keseluruhan dari hasil penelitian yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran yang didapat dari penelitian dari mulai merumuskan masalah sampai dengan selesai.