BAB I
PENDAHULUAN

1.1. Latar Belakang

Cloud computing adalah sebuah revolusi dari infrastruktur IT sebagai suatu layanan teknologi informasi yang dapat digunakan oleh pengguna dengan berbasis jaringan internet. Dimana suatu sumber daya dan penyediaan layanan komputasi disediakan untuk digunakan oleh komputer lain melalui jaringan internet (Mell dkk, 2011). Seiring dengan pesatnya adopsi teknologi *cloud computing,* terdapat isu keamanan yang menjadi masalah kritis pada penerapan teknologi *cloud computing*. Untuk itu dibutuhkan mekanisme pertahanan untuk mengamankan sumber daya terkait yang ada pada *cloud* megenai kerahasiaan, otentikasi, dan kontrol akses.

Pacific Rim Application and Grid Middleware Assembly (PRAGMA) adalah komunitas praktisi teknologi internasional di sekitar lingkar pasifik yang bertujuan untuk membangun kolaborasi berkelanjutan dengan memanfaatkan teknologi grid untuk memajukan penggunaan teknologi dalam riset ilmiah. PRAGMA terdiri dari kelompok-kelompok internasional berskala kecil hingga menengah untuk membuat kemajuan pesat dalam melakukan penilitian dan pendidikan dengan menyediakan infrastruktur dan mengembangkan *cyber infrastructure.* PRAGMA memiliki *cyber infrastructure* seperti *cloud server.* Dibutuhkan mekanisme pertahanan untuk mengamankan *cloud server* pada PRAGMA dari ancaman keamanan.

Isu Keamanan terkait pemanfaatan *cloud* di antaranya adalah *flooding attacks, browser attack, wrapping attack, malware injection attack,* dan *distributed denial of service* (DDoS). Serangan DDoS merupakana serangan yang sering dijumpai pada lingkup *cloud* (Singh, 2016). Serangan menggunakan konsep yang mirip dengan DoS namun pada pelancaran serangan DDoS dilakukan dengan lebih dari satu komputer. DDoS memiliki dampak yang beraneka ragam, tergantung dari seberapa besar tingkat serangan yang diterima (Elmustafa, 2015).

Serangan *distributed denial-of-service* (DDoS) pada *cloud computing* adalah salah satu masalah keamanan utama pada *cloud computing*. Serangan DDoS memiliki konsep yang sangat sederhana, yaitu membuat lalu lintas *server* berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari user lain. Dengan mengirimkan *request ke server* secara terus menerus dengan transaksi data yang besar (Gupta dkk, 2016). Serangan

ini lebih berbahaya daripada serangan lain dikarenakan serangan DDoS sulit untuk dideteksi dan memprediksi target serangan. Banyak perusahaan dan institusi yang menjadi target serangan DDoS mengalami kerugian finansial dan citra perusahaan atau institusi tersebut menjadi tercemar dikarenakan website yang digunakan untuk operasional mereka tidak dapat diakses.

Intrusion Detection System (IDS) merupakan sebagai salah satu solusi keaamanan pada jaringan. IDS memiliki beberapa keunggulan dibandingkan alat keamanan lainnya. Menurut Steven A. Hofmeyr dalam jurnalnya yang berjudul *Implementasi Intrusion Detection using Sequences of System Calls,* salah satu mekanisme keamanan IDS adalah dengan melakukan asumsi bahwa sistem dalam keadaan tidak aman, dengan begitu IDS akan melakukan pendeteksian dengan memantau dan menganalisa trafik degan pola yang aneh pada sistem (Hofmeyr, 1998).

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah hal yang sangat penting untuk dijaga. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak. Implementasi Suricata dapat mencegah percobaan tindakan ilegal terhadap sistem.

Keamanan adalah ketenangan dalam jiwa, kehormatan, harta dan aset-aset, perjalanan, dan lain sebagainya. Nikmat terbaik dalam Islam adalah adanya rasa aman, maka dari itu ujian yang pertama kali disebutkan dalam Al-Qur'an adalah ujian rasa takut (Sada, H. J., 2017) sebagaimana disebutkan dalam firman Allah SWT:

وَلَنَبْلُوَنَّكُمْ بِشَيْءٍ مِّنَ الْخَوْفِ وَالْجُوْعِ وَنَقْصٍ مِّنَ الْاَمْوَالِ وَالْاَنْفُسِ وَالثَّمَرٰتِۗ وَبَشِّرِ الصّٰبِرِيْنَ

Artinya: *"Dan sungguh akan Kami berikan cobaan kepadamu, dengan sedikit ketakutan, kelaparan, kekurangan harta, jiwa dan buah-buahan."* (QS. Al-Baqarah: 155)

Dari Abu Hurairah RA, Rasulullah SAW bersabda (Sada, H. J., 2017),

الْمُسْلِمُ مَنْ سَلِمَ النَّاسُ مِنْ لِسَانِهِ وَيَدِهِ وَالْمُؤْمِنُ مَنْ أَمِنَهُ النَّاسُ عَلَى دِمَائِهِمْ وَأَمْوَالِهِمْ

Artinya: "*Seorang Muslim adalah orang yang sanggup menjamin keselamatan orang-orang Muslim lainnya dari gangguan lisan dan tangannya, sedangkan seorang mukmin adalah orang yang seluruh manusia merasa aman darah dan harta mereka dari (gangguan) nya."* (HR. Muslim: Shahiihul Jaami 6709)

Berdasarkan ayat Al-Qur'an dan hadits di atas, dapat disimpulkan bahwa rasa aman lebih baik dari nikmat sehat dan waktu luang. Selain itu, terdapat perintah bagi kaum muslimin untuk selalu menjaga rasa aman dan hartanya dari gangguan ataupun ancaman dari luar. Dikarenakan mekanisme Suricata ini dapat mencegah dan melindungi sistem dari ancaman keamanan, dapat diibaratkan sebagai suatu cara untuk melindungi harta benda dari gangguan orang lain sebagaimana dianjurkan di dalam Islam.

1.2. Perumusan Masalah

Berdasarkan latar belakang di atas, maka dapat disimpulkan perumusan masalah penelitian ini yaitu, sebagai berikut:

a) Bagaimana Suricata menangani serangan DDoS (*distributed denial of serveice)* untuk *Cloud* PRAGMA?
b) Bagaimana hasil pengujian Suricata dalam mengatasi serangan DDoS?
c) Bagaimanan pandangan Islam terhadap dampak serangan DDoS?

1.3. Tujuan Penelitian

a) Melakukan implementasi Suricata sebagai metode pengamanan *cloud* PRAGMA dari serangan DDoS
b) Melakukan pengujian Suricata sebagai *Intrusion Detection System* dan *IpTables* sebagai *Intrusion Prevention System*
c) Mengetahui landasan hukum dan pandangan Islam terkait uji keamanan

1.4. Manfaat Penelitian

a) Mengetahui mekanisme serangan DDoS dan metode pengamanannya melalui Suricata untuk mencegah serangan DDoS bagi *cloud* PRAGMA
b) Mengetahui pandangan Islam terhadap penggunaan teknologi yang dilakukan

1.5. Batasan Masalah

a) Eksperimen dilakukan menggunakan *cloud* PRAGMA sebagai wadah pengujian
b) Metode penyerangan DDoS menggunakan *script* Slowloris yang dapat mengirimkan paket dalam jumlah acak secara terus menerus
c) Mekanisme pertahanan menggunakan Suricata sebagai *Intrusion Detection System* dan *IpTables* sebagai *Intrusion Prevention System*
d) Pengujian dilakukan berdasarkan skenario yang telah dibuat