BAB 1

PENDAHULUAN

1.1 Latar Belakang

Cloud computing adalah suatu paradigma baru dalam menggunakan sumber daya dan penyediaan layanan komputasi. *Cloud computing* memanfaatkan layanan internet sebagai pusat server yang bersifat virtual dengan tujuan pemeliharaan data dan aplikasi. Hal ini dikarenakan *cloud computing* melalui konsep vitualisasi, standarisasi dan fitur mendasar lainnya dapat mengurangi biaya Teknologi Informasi (TI). Pengguna *cloud* tidak memerlukan infrastruktur dan sumber daya komputasi lainnya untuk melakukan aktivitas komputasi (Singh, 2016).

Adaptasi *cloud computing* ke dalam *e-health* (penggunaan teknologi informasi dan komunikasi pada bidang kesehatan) dapat memperbaiki layanan kesehatan dan dapat membantu penelitian dibidang kesehatan serta dapat mengubah paradigma penggunaan teknologi informasi dalam bidang kesehatan (Kuo, 2011). Beberapa negara sudah menggunakan *cloud computing* dalam bidang *e-health*, misalnya Jerman (Löhr, Sadeghi, & Winandy, 2010) dan Taiwan (Lu, Ranjan, & Strazdins, 2015). Jerman menggunakan kartu elektronik untuk kesehatan (*electronic Health Card* (eHC)) yang berisi informasi administratif pasien dan digunakan untuk mengakses dan menyimpan data pasien di *e-health cloud* (Löhr et al., 2010). Taiwan menggunakan sistem yang hampir sama dengan Jerman dengan media electronik *Medical Record Template* (TMT) (Lu, 2015).

Keamanan menjadi tantangan yang paling kritis dalam implementasi *cloud compuitng* di bidang *e-health* (Rodrigues, 2016). Keamanan menjadi salah satu teknologi yang perlu diperhatikan ketika suatu sistem yang terkoneksi dengan system jaringan komputer menjadi hal yang sangat krusial. Pada saat ini kebutuhan manusia sangat tergantung dengan adanya informasi ataupun data, khususnya informasi atau data digital. Semakin besar kebutuhan adanya informasi semakin meningkat pula insiden atau gangguan keamanan terhadap sistem jaringan yang meningkat tajam. Hal ini umumnya terjadi dikarenakan masih kurangnya

kepedulian terhadap keamanan sebuah sistem khususnya pada infrastruktur *hardware* jaringan komputer yang masih sangat kurang. Keamanan jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Teknologi keamanan konvensional seperti *firewall* dan *IDS* (*Intrusion Detection System*) hanya saja masih memiliki kelemahan. Kebanyakan IDS sulit membedakan antara aktivitas legal dengan trafik *malicious.*

Isu keamanan terkait pemanfaatan cloud di antaranya adalah flooding attacks, browser attacks, wrapping attack, malware-injection attacks, dan distributed denial of service (DDoS). Serangan DDoS merupakan serangan yang sering dijumpai pada cloud (Singh, 2016). Serangan ini memililiki dampak yang beraneka ragam, tergantung dari seberapa besar tingkat serangan yang diterima (Choi, 2010).

Salah satu metode pencegahan terhadap DDoS adalah mennggunakan Suricata. Suricata memeriksa lalu lintas jaringan menggunakan aturan dan signature language yang kuat dan luas untuk mendeteksi ancaman yang kompleks. Alat ini dapat dikonfigurasi untuk beroperasi dalam tiga mode berbeda : sniffer mode, packet logger, dan network IDS mode. untuk Serangan yang akan dilancarkan adalah tipe DDoS yaitu Slowris.

Teknologi virtualisasi yang ada saat ini sangat banyak, salah satunya adalah Proxmox VE (*Virtual Environment*) yang merupakan Sistem Operasi *Open Source* virtualisasi yang berbasiskan Linux dan dapat dipergunakan untuk membangun *Private Cloud* dengan berbagai Platform Sistem Operasi.

Pada skripsi ini mengimplementasikan Suricata pada server cloud Proxmox sebagai IDS (Intrusion Detection System) sehingga dapat melakukan pencegahan dari attacker pada jaringan server cloud. Suricata dikombinasikan dengan firewall Iptables sehingga *firewall Iptables* dapat digunakan untuk memblok serangan DDoS sehingga dapat membantu pertahanan *firewall* di *e-health cloud.* Selain itu, juga akan dikaji penggunaan mekanisme Suricata untuk model *e-health cloud* Indoneisa menurut pandangan Islam.

Pandangan Islam terhadap metode Suricata ini dianggap sebagai upaya dalam pencegahan untuk melindungi harta benda dari hal buruk. Tujuan menggunakan Suricata ini dilihat menurut pandangan Islam merupakan tindakan *ikhtiar* karena berusaha untuk menjaga harta atau titipan dengan sebaik-baiknya semata-mata mengharapkan ridho dan pahala dari Allah SWT (Masrur, 2017). Dalam Islam, menggunakan Suricata untuk model *e-health cloud security* merupakan salah satu langkah dalam menuntut ilmu dibidang sains dan teknologi. Rasulullah SAW di dalam haditsnya menjelaskan bahwa menuntut ilmu bagi seorang muslim merupakan suatu kewajiban dan akan bernilai pahala bagi yang melakukannya (HR Ibnu Majah).

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka dapat disimpulkan perumusan masalah adalah sebagai berikut :

a. Bagaimana rancangan topologi yang akan diimplementasikan ?
b. Bagaimana cara Suricata mendeteksi serangan DDoS TCP *flood* ?
c. Bagaimana hasil pengujian setelah berhasil mengatasi serangan DDoS ?
d. Parameter apa saja yang dapat digunakan untuk mendeteksi serangan DDoS?
e. Bagaimana pandangan Islam terhadap implementasi suricata pada *cloud server* Proxmox ?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

a. Implementasi mekanisme *virtual firewall* untuk model *e-health cloud* Indonesia.
b. Pengujian terhadap jumlah paket yang dapat membuat server tidak dapat diakses.
c. Mengkaji penggunaan mekanisme Suricata untuk model *e-health cloud* Indonesia menurut agama Islam.

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah :

a. Memberikan dan mempelajari rekomendasi metode untuk mencegah serangan DDoS.
b. Mengetahui keamanan yang dapat diterapkan pada *Cloud Server*.
c. Membantu *administrator* dalam merekomendasi metode untuk mencegah serangan DDoS.
d. Mengetahui pandangan Islam terhadap penggunaan Suricata pada *cloud server* Proxmox.

1.5 Batasan Masalah

Adapun batasan masalah yang dilakukan pada penelitian ini adalah :

a. Eksperimen ini dibangun dengan menggunakan VMware Workstation sebagai simulasi.
b. Metode penyerangan DDoS menggunakan *script* Slowris yang dapat mengririm paket dalam jumlah acak secara terus menerus.
c. Topologi yang digunakan mengacu pada *Indonesian e-Health Cloud Deployment Model.*
d. *Router virtual* dan *server* virtual dibangun menggunakan virtualisasi pada *node* Proxmox VE.
e. Pengujian dilakukan berdasarkan scenario yang dibuat.