BAB 1
PENDAHULUAN

1.1 Latar Belakang

Teknologi *Cloud Computing* adalah paradigma baru dalam penyampaian layanan komputasi (Kurniawan, 2015). *Cloud* memanfaatkan teknologi layanan internet menggunakan pusat server yang bersifat virtual dengan tujuan pemeliharaan data dan aplikasi. Keberadaan *cloud* menimbulkan perubahan dalam cara kerja sistem teknologi informasi dimana sistem *cloud computing* yang berupa sistem *resource* yang dapat diakses secara *online* sehingga sangat fleksibel terhadap penggunanya. *Cloud computing* memiliki banyak kelebihan dibandingkan dengan sistem konvensional. Pengguna *cloud* tidak memerlukan infrastruktur dan sumber daya komputasi lainnya untuk melakukan aktivitas komputasi.

Adaptasi *cloud computing* ke dalam *e-health* (penggunaan teknologi informasi dan komunikasi pada bidang kesehatan) menjadi sangat menarik karena *cloud* menjadi model baru yang memungkinkan kemudahan dalam akses data medis, dan peluang untuk bisnis. Namun mereka juga menanggung risiko dan dampak sehubung dengan aspek keamanan dan privasi yang perlu ditangani secara hati-hati saat di terapkan *e-health cloud*. *E-health* merupakan penggunaan teknologi informasi dan komunikasi pada bidang kesehatan. *Telemedicine* salah satu implementasian *e-health cloud* yakni pelayanan di bidang kesehatan jarak jauh. *Telemedicine* didefinisikan sebagai transfer data medis elektronik dari satu lokasi ke lokasi lainnya via *online* (Jamil dkk, 2015). *E-health* merupakan aplikasi berbasis TIK (teknologi informasi dan komunikasi) yang berkaitan dengan industry pelayanan kesehatan serta bertujuan untuk meningkatkan akses, efisiensi, efektivitas, serta kualitas proses medis.

Keamanan menjadi salah satu komponen yang krusial untuk diperhatikan ketika suatu sistem terkoneksi dengan sistem jaringan komputer. Dalam pemanfaatan *cloud* terdapat isu keamanan di antaranya adalah *Ransomware, SQL Injection, Spoofing, Packet Sniffing, Port Scanning, ICMP flood, UDP flood,* dan *distributed denial of service* (DDoS). Serangan *port scanning* dan *DDoS* merupakan serangan yang sering dijumpai di antara serangan lainnya terhadap *cloud*. Pada dasarnya

mekanisme *DDoS* sama dengan *denial of service* (DOS) namun serangannya lebih terstruktur dan memilki dampak yang jauh lebih besar dibandingkan dengan *DOS*. Serangan ini dapat mengakibatkan *server* menjadi *down* dan mengakibatkan *system error*. Teknologi sistem keamanan konvensional seperti *firewall* dan *IDS* (*intrusion detection system*) masih memiliki kelemahan. Kebanyakan *IDS* sulit membedakan aktivitas legal dengan trafik yang mencurigakan. Misalnya, posting dari BugTraq tentang bahaya kode *exploit*, dianggap oleh IDS sebagai *buffer overlow* karena polanya cocok.

Salah satu metode optimalisasi dan pencegahan dini terhadap serangan *DDoS* adalah dengan *Honeypot*. *Honeypot* merupakan sebuah sistem yang berfungsi untuk menjebak pengguna yang bertujuan buruk. *Honeypot* sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (Cahyanto dkk, 2013). Dengan *Honeypot* layanan *cloud computing* dapat terhindar dari berbagai serangan. *Honeypot* dapat mengumpulkan informasi mengenai penyerang yang meliputi identitas dan aktifitas yang dilakukan oleh si penyerang dalam upaya melakukan serangan ke layanan *cloud computing*. Dari informasi yang diberikan oleh *honeypot* penyedia layanan *cloud* dapat melakukan peningkatan pengamanan pada layanan *cloud computing* yang dimilikinya (Agustino dkk, 2017).

Honeypot tersebut melayani serangan yang dilakukan *attacker* dalam melakukan penetrasi terhadap *server*. Penerapan *honeypot* bertujuan untuk mendapatkan data-data dari para penyerang tentang bagaimana cara mereka masuk ke dalam sistem. Dengan *Honeypot* dibuat *server* bayangan atau palsu (*fake*) dimana menyerupai sistem aslinya melakukan analisis, hasilnya sistem *server* terlindungi dan para penyusup dapat dialihkan ke *server* palsu dan data di *server* asli lebih aman. Dengan menggunakan *software Honeyd-Viz* melalui web interface, Admin Jaringan dapat melihat, menganalisa, dan mempelajari serangan dari *attacker* terhadap sistem (Husnan, 2013).

Cloud computing merupakan penyedia sumber daya teknologi informasi yang memanfaatkan sumber daya *virtual* dalam mengelola sumber daya komputasi dan penyimpanan data. Namun di sisi lain penggunaan *cloud computing* memiliki permasalahan yaitu di sisi keamanan (Agustino dkk, 2017).

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.

Pandangan Islam terhadap metode *Honeypot* dianggap sebagai upaya dalam pencegahan untuk melindungi harta benda dari hal buruk. Menurut Islam dalam menggunakan *Honeypot* merupakan tindakan *Ikhtiar* karena kewajiban manusia ialah berusaha mencapainya dengan kemampuannya semaksimal mungkin. Firman Allah SWT.

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأۡكُلُوٓاْ أَمۡوَٰلَكُم بَيۡنَكُم
بِٱلۡبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٖ مِّنكُمۡۚ وَلَا تَقۡتُلُوٓاْ
أَنفُسَكُمۡۚ إِنَّ ٱللَّهَ كَانَ بِكُمۡ رَحِيمٗا ٢٩

Artinya :

"Hai orang-orang yang beriman, janganlah kamu saling memakan harta sesamamu dengan jalan yang batil, kecuali dengan jalan perniagaan yang berlaku dengan suka sama-suka diantara kamu. Dan janganlah kamu membunuh dirimu; Sesungguhnya Allah adalah Maha Penyayang kepadamu" (Q.S. An-Nissa (4) : 29)

Mengembangkan ilmu dan teknologi itu merupakan tuntutan untuk berbuat sesuatu dengan sarana teknologi. Akan tetapi, karena pergeseran waktu dan perkembangan pemikiran, antara agama dan sains seakan akan terkotak-kotak. Agama tanpa dukungan sains akan menjadi tidak mengakar pada realitas dan penalaran. Sedangkan sains yang tidak dilandasi dasar - dasar ilmu agama akan berkembang menjadi liar dan menimbulkan dampak merusak. Karena itulah timbulnya islamisasi sains pada hakikatnya merupakan keinginan untuk mengintegrasikan agama dan sains dan memandang sains sebagai upaya untuk membuka sunnatullah (Purwanigrum, 2017). Menurut (Qathrun dkk, 2014) Dalam Islam sendiri menuntut ilmu bukan hanya sekedar imbauan belaka, tapi sudah dijadikan kewajiban bagi setiap umat manusia. Hal ini terbukti begitu banyaknya perintah yang terdapat dalam Al-Qur'an ataupun hadits yang membahas tentang menuntut ilmu, penting

penguasaan ilmu serta berbagai hal yang mengarah kepada kewajiban mencari ilmu. Sebagaimana hadis Rasulullah SAW :

طَلَبُ الْعِلْمِ فَرِيْضَةٌ عَلَى كُلِّ مُسْلِمٍ

Artinya :

"Menuntut ilmu itu wajib atas setiap muslim" (HR. Ibnu Majah).

Pada skripsi ini penulis mengimplementasikan mekanisme *Honeypot* pada model *e-health cloud security* untuk optimalisasi keamanan jaringan. Dengan pengimplementasian tersebut dapat dilakukan deteksi dan monitoring *server*, menguji serangan DDoS serta mengetahui metode yang digunakan dalam menyerang suatu sistem sehingga dapat dilakukan tindakan pelindungan terhadap sistem. Selain itu, akan dilakukan terhadap kajian penggunaan *Honeypot* untuk model *e-health cloud* Indonesia menurut pandangan Islam.

1.2 Perumusan Masalah

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

a. Bagaimana ketahanan sistem *Honeypot* yang diimplementasikan pada model *e-health cloud* ketika *server* akan diserang *attacker*?
b. Bagaimana hasil pengujian setelah berhasil mendeteksi terhadap serangan DDos ?
c. Bagaimana pandangan Islam terhadap analisis dan implementasi *Honeypot* untuk model *e-health cloud security*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

a. Menguji *e-health cloud* Indonesia yang menggunakan *Honeypot* dengan *Honeyd* terhadap serangan *DDoS.*
b. Menguji kinerja terhadap paket SYN, *Port Scanning* dan Serangan DDoS lainnya yang dapat mempengaruhi server ke sistem *Honeypot.*
c. Mengkaji penggunaan mekanisme *Honeypot* dengan *Honeyd* untuk model *e-health cloud security* menurut pandangan Islam.

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah :

a. Membantu *administrator* jaringan dalam mengantisipasi serangan ke server.
b. Membantu *administrator* untuk melihat, menganalisis, dan mempelajari serangan terhadap sistem dengan menggunakan *software Honeyd-Viz* yang diterapkan pada *honeypot Honeyd.*
c. Mengetahui kinerja sistem *Honeypot* yang diserang dengan berbagai macam serangan *DDoS*
d. Memberikan rekomendasi metode untuk pencegahan dini terhadap serangan DDoS.

1.5 Batasan Masalah

Adapun batasan masalah yang dilakukan pada penelitian ini :

a. Simulasi dengan VMware Workstation.
b. Metode *Honeypot Honeyd* untuk mengatasi serangan DDoS.
c. Virtual *router* dan *server* dibangun menggunakan Proxmox VE.
d. Serangan: DDoS menggunakan *script* Slowloris dan *script* SYN *flooding attack* menggunakan *python* pada kali linux, serta penyerangan *port scanning.*
e. Hasil serangan divisualisasikan menggunakan *Honeyd-Viz*
f. Pengujian dilakukan berdasarkan skenario yang telah dibuat.