BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan internet dan pengembangan dari perangkat elektronik pintar mengarah kepada pengembangan dari sebuah prototype komputer baru yaitu IoT *(Internet of Things)*. IoT dianggap menjadi investasi masa depan internet yang bekerja pada komunikasi *Machine to Machine* (M2M) dan *Radio Frequency Identification* (RFID). Tujuan utama dari IoT *(Internet of Things)* adalah untuk memungkinkan pertukaran data yang aman antara perangkat dunia nyata dan aplikasi[1].

Internet of Things (IoT) telah menjadi cukup akrab dalam beberapa tahun terakhir. Banyaknya perangkat rutinitas sehari-hari semakin terhubung dengan Internet yang mencakup banyak kemampuan seperti penginderaan, otonomi dan kesadaran kontekstual. Perangkat IoT termasuk komputer pribadi, laptop, smartphone, tablet dan perangkat rumah yang tertanam lainnya. Jaringan interkoneksi pada *Internet of Things (IoT)* dapat menghubungkan berbagai objek yang memiliki identitas pengenal serta alamat IP, sehingga dapat saling berkomunkasi dan bertukar informasi data.

Karena banyaknya jumlah perangkat yang terhubung ke *Internet of Things* (IoT) pada akhirnya mendapat perhatian serangan *hacker* dalam melanggar mekanisme keamanan. Untuk menyelidiki serangan tersebut kita perlu menerapkan aspek forensik digital di *Internet of Things* (IoT) yang kita sebut dengan istilah IoT Forensik. Salah satu isu yang masih menjadi kelemahan dalam pengimplementasian *Internet of Things* (IoT) adalah masalah keamanan dan privasi[2].

Serangan terhadap keamanan *Internet of Things* (IoT) dapat mencakup serangan terhadap label *Radio Frequency Identification* (RFID), jaringan komunikasi maupun pada privasi data. Serangan *Flooding* menjadi salah satu bentuk serangan *Denial of Service* (DoS) terhadap jaringan perangkat *Internet of Things* (IoT) yang mengakibatkan suatu sistem akan terbanjiri oleh data – data secara terus menerus dalam waktu singkat dan juga mengakibatkan lalu lintas jaringan menjadi sangat padat[3].

Dalam penelitian ini implementasi framework *Generic Network Forensics* bertujuan melakukan investigasi forensik jaringan untuk mendeteksi serangan *flooding* pada perangkat *Internet of Things* (IoT).

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah penelitian diatas, diuraikan menjadi beberapa pertanyaan, antara lain :

1. Bagaimana mendeteksi serangan flooding pada perangkat Internet of Things (IoT) ?
2. Bagaimana mengimplementasi framework *Generic Network Forensics Process Model* untuk menemukan serangan *flooding* dari perangkat *Internet of Things* (IoT) ?

1.3 Batasan Masalah

Dalam penelitian ini Penulis membatasi masalah yang akan dibahas. Lingkup atau *scope* pembahasan meliputi :

1. Penelitian ini akan membatasi serangan flooding pada perangkat IoT hanya pada serangan SYN Flooding.
2. Fokus Penelitian ini hanya dilakukan proses forensik jaringan pada perangkat Internet of Things (IoT).

1.4 Tujuan Penelitian

Adapun tujuan penelitian sebagai berikut :

1. Untuk mendeteksi serangan flooding pada perangkat IoT yang digunakan.
2. Untuk mengetahui aktivitas yang terjadi pada perangkat IoT.
3. Menguji framework *Generic Network Forencis Process Model* untuk mendeteksi serangan flooding pada perangkat *Internet Of Things* (IoT)

1.5 Manfaat Penelitian

Setelah adanya penjabaran mengenai tujuan dari penelitian ini, maka penelitian ini juga memiliki manfaat yang dapat diambil. Manfaat dari penelitian yang dilakukan antara lain :

1. Memberi kontribusi terhadap pengembangan ilmu *Digital Forensics* khususnya tentang *Internet of Things (IoT) Forensics Device*, dengan memanfaatkan framework *Generic Network Forensic Model* untuk menenukan serangan *flooding* pada perangkat *Internet of Things* (IoT).
2. Mengetahui trafik dan log file pada perangkat *Internet of Things* (IoT).
3. Mengetahui proses forensik jaringan yang terjadi dalam *Digital Forensics Investigation* pada perangkat *Internet Of Things (IoT)*

1.6 Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian yang dibuat, maka dibuat sistematika penulisan pada penelitian ini :

BAB I PENDAHULUAN

Di bab ini menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat

penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan *digital forensics, network forensics model, flooding attack* dan

Forensic in Internet of Things (IoT) environment.

BAB III METODE PENELITIAN

Bab ini membahas tentang langlah-langkah penelitian dan gambaran umum langkah penyelesaian. Berisi tentang arsitektur forensik *Internet of Things* (IoT), tantangan forensik jaringan pada perangkat IoT dan pengujian model framework *Generic Network Forensik Process Model*.

BAB IV HASIL DAN PEMBAHASAN

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat, pengujian kinerja dan penentuan hasil analisa.

BAB V PENUTUP

Simpulan dan Saran, berisi tentang kesimpulan-kesimpulan dari hasil penelitian dan saran - saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan. asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.