Abstrak

Dengan meningkatnya perangkat yang tersambung ke Internet mendasari *Internet of Things* (IoT) tumbuh dengan cepat, namun banyak dari perangkat ini pada dasarnya tidak aman, terekspos bebas di Internet dan memungkinkan terjadi beragam serangan siber. Akhir-akhir ini, IoT telah dipengaruhi oleh berbagai *botnet* dengan aktivitas berbeda diantaranya adalah serangan *Distributed Denial of Service* (DDoS), *spamming*, *phising*, sampai dengan menginfeksi sistem lain. Dikarenakan *botnet* dengan serangan tersebut telah menjadi penyebab risiko keamanan yang cukup serius terhadap infrastruktur Internet selama bertahun-tahun, belum ada teknik *Network Forensics* yang dapat mengidentifikasi dan melacak tingkah laku botnet canggih sampai saat ini. Pada literatur lain terdapat penelitian yang telah menggunakan *Machine Learning* (ML) untuk melatih dan memvalidasi pemodelan untuk mendefinisikan serangan tersebut, akan tetapi masih menghasilkan kesalahan yang cukup tinggi dalam menyelidiki jejak botnet. Hal ini memotivasi pengembangan teknik baru untuk *Network Forensics* berdasarkan identifikasi aliran jaringan yang dapat melacak jejak aktivitas *botnet* yang di curigai. Berdasarkan hasil eksperimen didapatkan *Machine Learning* (ML) dipadukan dengan identifikasi aliran jaringan cukup efektif dan efisien dalam mengidentifikasi dan mengklasifikasi serangan dan jejak aktivitas *botnet* pada *Internet of Things* (IoT).

Kata kunci : internet of things, cyber attack, botnet, network forensics, machine learning.