1. Pendahuluan

Latar Belakang

Di era perkembangan teknologi saat ini sistem kamera pengawas (CCTV) telah banyak digunakan dalam sistem keamanan, dikarenakan kamera pengawas (CCTV) merupakan salah satu alat yang sangat diperlukan dalam meningkatkan keamanan. Dengan adanya kamera pengawas (CCTV) kita dapat mengetahui terjadinya tindak kriminal atau bahkan tindak kejahatan lainnya tanpa harus berada ditempat tersebut. Kamera pengawas (CCTV) juga sering digunakan sebagai salah satu bukti ketika hal-hal yang tidak diinginkan terjadi. Namun, meskipun penggunaan kamera pengawas (CCTV) bertujuan untuk meningkatkan keamanan tak sedikit pun tantangan yang dihadapi, kamera pengawas yang canggih akan memerlukan peralatan, data, serta bandwidth yang cukup besar [1]. Bukan hanya itu yang menjadi tantangan dari adanya kamera pengawas (CCTV), kamera pengawas (CCTV) juga menjadi salah satu sasaran terjadinya penyerangan, meskipun telah banyak peneliti yang mencoba untuk mewujudkan perlindungan privasi dalam kamera pengawas video (CCTV), namun relatif sedikit yang fokus untuk membangun sebuah keamanan pada sistem kamera pengawas video (CCTV) dari sebuah serangan *man-in-the-middle-attack* (MITM) [2].

Salah satu serangan *man-in-the-middle-attack* (MITM) yang terjadi pada kamera pengawas (CCTV) adalah serangan *video injection. Video injection* merupakan serangan dengan melakukan penyuntikkan video pada aliran video stream (CCTV) atau memutar ulang video pada aliran kamera pengawas (CCTV). Penyerangan *video injection* cukup berbahaya karena, dapat menyembunyikan bukti sebenarnya dan penyerangan *video injection* telah melanggar model standar dalam keamanan informasi yang dikenal dengan CIA Triad. Kasus ini melanggar Confidentiality dan Integrity dari sebuah data dimana seorang penyerang dapat mengakses rekaman video kamera pengawas yang seharusnya bersifat rahasia dan mengubah isi informasi yang terpercaya pada sebuah rekaman kamera pengawas (CCTV) [3]. Salah satu cara untuk mengurangi adanya penyerangan injection adalah melakukan deteksi serangan dengan memanfaatkan *ensemble learning*. *Ensemble learning* merupakan salah satu algoritma gabungan antara beberapa model algoritma lainnya atau menggunakan satu metode algoritma [4]. Inilah yang mengilhami kami membuat model deteksi serangan *video injection* menggunakan *ensemble learning bagging* dengan menggunakan estimator *random forest* dan kemudian akan dibandingkan dengan menggunakan estimator *support vector machine* (SVM).

Penelitian yang dilakukan oleh Hoang Ngoc Thanh dkk bertujuan untuk mendeteksi serangan *denial of service* (DoS) sehingga dapat mengurangi terjadinya penyerangan DoS dengan menganalisis serta mengevaluasi kinerja serangan DoS dengan menggunakan beberapa metode klasifikasi *ensemble*, diantaranya adalah *bagging*, *adaboost, stacking, decorate, random forest* dan *voting* tunggal. Metode dengan hasil yang terbaik yaitu menggunakan teknik *ensemble stacking* dengan hasil kinerja *f-measure* sebesar 99.28% dibandingkan dengan teknik *ensemble* lainnya [5]. Penelitian selanjutnya yang dilakukan oleh Jin Ye dkk mendeteksi serangan DDoS pada bidang keamanan jaringan. Data yang digunakan pada penelitian ini menggunakan data langsung dengan menggunakan *Openflow* dimana data informasi tabel dikirim dan nilainya akan diekstraksi menjadi nilai karakteristik, yang kemudian nilai karakteristik akan diklasifikasi dengan menggunakan algoritma berbasis *support vector machine* (SVM) untuk membedakan lalu lintas normal dengan lalu lintas abnormal. Dalam penelitian ini menggunakan metode klasifikasi algoritma *support vector machine* (SVM) dengan nilai akurasi sebesar 95.24% [6].

Topik dan Batasannya

Berdasarkan latar belakang permasalahan yang telah diuraikan diatas, topik penelitian yang dikerjakan pada tugas akhir ini adalah bagaimana cara membagun sistem pendeteksi serangan *video injection* dengan algoritma *random forest* dan bagaimana performansi dari penerapan *ensemble learning bagging* algoritma *random forest* dengan algoritma *support vector machine* (SVM).

Batasan masalah dari penelitian tugas akhir ini diantaranya adalah Dataset yang digunakan bersumber dari *website Kaggle* oleh Kitsune *Network Attack Dataset* dengan pengambilan data pada tahun 2018 dan Dataset yang digunakan menggunakan tiga dataset berbeda diantaranya, dataset *Video Injection, Active Wiretap* dan ARP MiTM berupa rekaman paket data yang telah di extrak menggunakan ekstraktor fitur *AfterImage* dan siap sebagai data pembelajaran *machine learning* pada sebuah jaringan sistem keamanan CCTV.

Tujuan

Penelitian ini bertujuan untuk melakukan pendeteksi serangan *video injection* menggunakan metode *ensemble learning bagging* dengan algoritma *random forest* dan membandingkan performansi *ensemble learning bagging* algoritma *random forest* dengan algoritma *support vector machine* (SVM).

Organisasi Tulisan

Organisasi penulisan pada penelitian ini diantaranya adalah bagian ke 1 yang berisi latar belakang, topik, batasan, dan tujuan. bagian ke 2 menjelaskan studi terkait. bagian ke 3 dijelaskan detail sistem yang dibangun menggunakan *ensemble learning bagging* dengan algoritma *random forest*. Pada bagian ke 4 berisi tentang hasil dan diskusi. Pada bagian ke 5 berisi tentang kesimpulan.