1. Pendahuluan

Latar Belakang

Perlindungan dan pemantauan keamanan *website* kampus semakin penting seiring dengan peningkatan penggunaan teknologi dalam pembelajaran. Namun, saat ini kurangnya perhatian terhadap aspek keamanan jaringan. Hal ini membuat layanan *web server* di lingkungan kampus menjadi rentan terhadap gangguan yang dilakukan oleh pihak yang tidak berwenang seperti aktivitas mencurigakan, serangan siber, atau perubahan signifikan dalam pola akses ke *website* kampus.

Pada saat *website* pada *web server* mengalami gangguan, seorang administrator akan memeriksa *log* untuk mengetahui apa dan darimana serangan tersebut berasal dan data peretas akan diketahui dengan cara melihat dari alamat IP yang dipakai untuk mengakses *website*[1]. Dibutuhkan adanya upaya untuk menjaga dan menjamin keamanan informasi terhadap layanan yang berada di *web server*[2]. Pentingnya memiliki pencatatan *log web server* secara *real-time* yang mencatat semua aktivitas layanan yang berjalan di *web server*[3].

Untuk menganalisis data *log web server*, diperlukannya *log monitoring system*[4]. *Security Information Event and Managemen (SIEM)* merupakan sistem informasi yang digunakn untuk mengumpulkan data *log* yang nantinya menghasilkan keluaran visualisasi *log* monitoring untuk mempermudah pembacaan informasi *log*[5]. Pemilihan algoritma merupakan hal yang dasar yang diperlukan dalam mengimplementasikan teknologi *Security Informasion Event and Management (SIEM)*[5].

Banyak algoritma yang bisa diterapkan dalam mengelompokkan data, salah satunya yaitu algoritma *Clustering*. Pemilihan metode *Clustering* berdasarkan kemampuannya untuk mengelompokkan data. Algoritma *K-Means Clustering* digunakan untuk mengelompokkan data berdasarkan kedekatan satu sama lain sesuai jarak *Euclidean* [3]. *K-Means Clustering* termasuk dalam *unsupervised-machine learning*, metode untuk membagi satu set data menjadi beberapa kelompok yang memiliki kemiripan fitur [6]. Algoritma DBSCAN mengelompokkan data berdasarkan kepadatan. DBSCAN mampu mengidentifikasi kelompok dengan berbagai ukuran dan bentuk serta mendeteksi *Noise* dalam sejumlah besar data yang mengandung *Noise* dan *Outlier* [16].

Oleh karena itu, Tugas Akhir ini bertujuan untuk mengatasi masalah tersebut dengan mengembangkan sistem yang mampu memantau aktivitas pengunjung *website* kampus dan mendeteksi pola anomali. Sistem ini menggunakan metode *Clustering* untuk mengelompokkan data *log* berdasarkan atributnya seperti *Status Code*, URL, dan *Response Size*. Digunakannya algoritma *K-Means Clustering* dan DBSCAN dengan tujuan untuk menguji efektivitasnya dalam mendeteksi anomali pada *web server*. Pada tugas akhir ini akan mengevaluasi apakah *K-Means Clustering* dan DBSCAN mampu mengungkapkan pola yang mencurigakan dalam *log web server*. Hasil dari Tugas Akhir ini dapat membantu mengidentifikasi pola yang tidak biasa dalam data *log web server* dan menguji efektivitas dari metode *Clustering* dengan matriks evaluasi *Silhouette Score*.

Topik dan Batasannya

Pada tugas akhir ini memfokuskan pada analisis data *log web server* untuk meningkatkan keamanan jaringan dan melindungi data sensitif, terutama dalam konteks lingkungan kampus Universitas Telkom Surabaya dengan penelitian yang difokuskan pada *web server bis-sby.telkomuniversity.ac.id*. Bagaimana analisis data *log web server* dapat membantu mengidentifikasi aktivitas yang tidak biasa, serta bagaimana algortima *K-Means Clustering* dan algoritma DBSCAN dapat diterapkan untuk mengelompokkan data *log web server* dan mengidentifikasi pola anomali.

Namun dalam tugas akhir ini terdapat batasan yang perlu diperhatikan. Tugas Akhir ini dibatasi pada deteksi anomali dalam data *log web server*, khususnya pada aktivitas *Status Code*, URL, dan *Response Size* yang diatas rata-rata dari data *log web server* selama 7 hari. Selain itu, tidak ada kemampuan untuk melakukan monitoring secara *real-time* karena keterbatasan akses langsung ke *server* kampus Universitas Telkom Surabaya. Dengan memperhatikan batasan ini, diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan jaringan *web server* dengan memonitoring data *log* dan mendeteksi anomali di lingkungan kampus Universitas Telkom Surabaya.

Tujuan

Tujuan dari tugas akhir ini untuk merancang dan mengimplementasikan sistem monitoring untuk mengumpulkan dan menganalisis data *log* dari *web server* selama periode waktu 7 hari. Mengidentifikasi pola atau aktivitas yang tidak biasa dalam aktivitas pengunjung *website* kampus Universitas Telkom Surabaya menggunakan algoritma *K-Means Clustering* dan algoritma DBSCAN berdasarkan jarak antar *cluster*, melabeli data anomali berdasarkan *Status Code*, URL, dan *Response Size* yang diatas rata-rata dari data *log web server* selama 7 hari. Dengan melabeli hasil deteksi anomali, dapat membantu administrator jaringan dalam mengidentifikasi jenis anomali yang ada.

Selain itu, tugas akhir ini bertujuan untuk mengetahui performa *Clustering* menggunakan matriks evaluasi *Silhouette Score* untuk memastikan akurasi dan efektivitas pengelompokan data *log web server*. Dengan demikian,

tugas akhir ini dapat memberikan kontribusi yang berarti dalam mengamankan infrastruktur teknologi informasi di lingkungan kampus serta menjaga kerahasiaan dan integritas data yang tersimpan.

Organisasi Tulisan

Pada tugas akhir ini, dibuat dan disusun dengan organisasi tulisan sebagai berikut:

- Pendahuluan, Pada bagian ini menjelaskan mengenai apa saja yang mendasari tugas akhir ini, tujuan, serta apa tugas akhir ini.
- Studi Terkait, Pada bagian ini menjelaskan mengenai cara tugas akhir ini dibuat dengan menggunakan beberapa referensi yang digunakan sebagai pengembangan dari tugas akhir ini.
- Sistem yang Dibangun, Pada bagian ini menjelaskan mengenai penyusunan sistem yang dibangun dan diimplementasikan pada tugas akhir ini.
- Evaluasi, Pada bagian ini menjelaskan mengenai hasil dan proses analisa dari hasil yang diperoleh dari tugas akhir ini.
- Kesimpulan, Pada bagian ini menjelaskan mengenai apa saja yang dapat disimpulkan dari hasil tugas akhir ini.