**JUDUL PROYEK AKHIR**

|  |  |  |
| --- | --- | --- |
| 1. Nama Lengkap | : | Dimas Rizky H.P. |
| 2. NRP | : | 2110141011 |
| 3. Kelas | : | 3 D4 Informatika - A |
| 4. Jurusan/Program Studi | : | D4 Teknik Informatika |
| 5. Judul Proyek Akhir | : | Implementasi Log Report Clustering Menggunakan Metode Stream Clustering Untuk Analisa Log Data Pada Aplikasi Mata Garuda |

6. Deskripsi Proyek Akhir :

* Latar belakang Proyek akhir

Mata Garuda merupakan *IDS (Intrusion Detection System)* yang memonitor lalu lintas data pada jaringan internet yang ada di Indonesia. Mata Garuda akan melaporkan suatu kejadian yang cirinya telah didefinisikan dalam sebuah rule. Kejadian-kejadian tersebut didapatkan melalui sensor yang terpasang di netiap *Network Access Point* yang ada di Indonesia. Sensor tersebut berfungsi untuk mengambil paket lalu meneruskannya ke *defense center*. Setiap harinya terdapat puluhan juta packet yang ditangkap oleh sensor Mata Garuda dan dengan terdeteksi rata-rata 2 juta serangan dideteksi per harinya.

Dengan Semakin berkembangnya teknologi dan semakin banyaknya pengguna internet di Indonesia maka akan semakin besar pula lalu lintas data yang melewati sensor mata garuda. Dengan semakin besarnya lalu lintas data pada jaringan akan menyebabkan semakin banyaknya *event* yang harus diproses dan dianalisa oleh *defense center* Mata Garuda. Hal ini berpengaruh secara langsung dalam kecepatan Mata Garuda dalam menganlisa data lalu lintas tersebut. Oleh karena itu, pengembangan arsitektur sistem Mata Garuda harus dilakukan agar dapat sesuai dengan kondisi sekarang

* Permasalahan Proyek akhir

Dalam melakukan analisa terhadap log file yang dihasilkan oleh Mata Garuda memerlukan adanya pendekatan *machine learning* berupa *clustering* data yang sudah ada. Clustering pada umumnya menuntut agar data disimpan pada sebuah tempat penyimpanan terlebih dahulu untuk nantinya akan di proses atau di *cluster* beberapa waktu kemudian untuk menghasilkan sebuah analisa. Hal ini akan memakan waktu yang sangat lama jika diterapkan pada Mata Garuda yang memiliki jutaan data.

* Tujuan Proyek akhir

Pada penelitian ini mengajukan suatu pendekatan untuk melakukan proses analisa berupa *clustering* pada log data Mata Garuda dengan menyediakan suatu fitur yang memungkinkan proses analisa berjalan lebih cepat dengan menggunakan metode *stream clustering.*

* Referensi

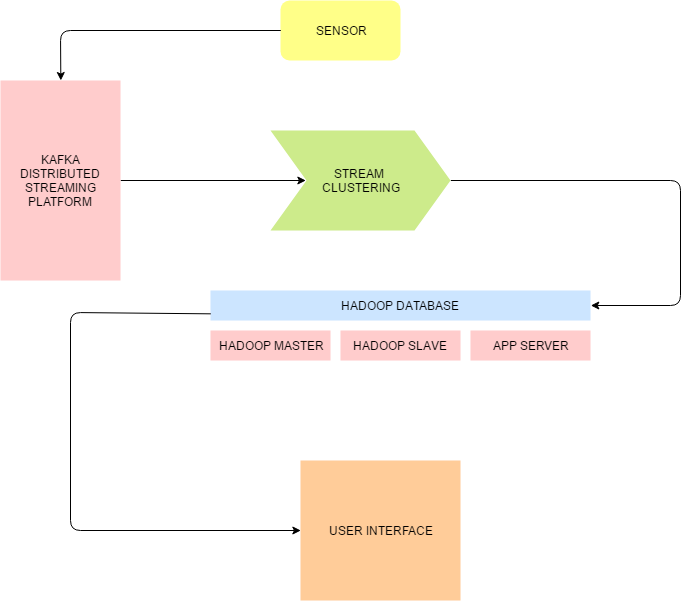
Pembuatan tugas akhir ini mengacu pada beberapa referensi yaitu :

1. Antonio L. Severien. *Scalable Distributed Real-Time Clustering for Big Data Streams*, 2013.
2. Wathiq Laftah Al-Yaseen, Zulaiha Ali Othman, dan Mohd Zakree Ahmad Nazri. *Real-Time Intrusion Detection System Using Multi-agent System*, 2016.

* Metode yang digunakan

*Data stream clustering* adalah metode pengelompokan data yang datang secara terus menerus seperti catatan telepon, data multimedia, transaksi keuangan dan lainnya

* Rancangan Diagram Sistem



* Penjelasan dan Deskripsi Diagram Sistem

1. Sensor

Merupakan sensor mata garuda untuk mendapatkan input packet yang keluar masuk pada interface sensor mata garuda. Selain itu juga untuk mendeteksi adanya kejadian yang sudah didefinisikan pada rule yang ada

1. Kafka Distributed Streaming Platform

Merupakan *distributed platform* untuk membagun jalur data *streaming* yang berjalan secara *real-time*

1. Stream Clustering

Merupakan metode pengelompokan data yang datang secara terus menerus tanpa putus.

1. Hadoop Database

Hadoop adalah framework perangkat lunak berbasis java yang berfungsi untuk mengolah data yang besar secara terdistribusi dan berjalan di atas *cluster* yang terdiri dari beberapa komputer yang saling terhubung

1. User Interface Mata Garuda

Merupakan user interface dari aplikasi Mata Garuda yang berisi menu fitur fitur dari mata garuda, laporan kejadian, analisa kejadian, dan lainnya.

* Nama Calon Dosen Pembimbing :

Pembimbing 1 : Ferry Astika Saputra, S.T, M.Sc.

Surabaya, 8 Mei 2017

Dimas Rizky H.P.

2110141011