1. Pendahuluan

Anomaly detection (atau yang juga bisa disebut *outlier* detection) adalah sebuah metode yang diaplikasikan untuk menemukan data yang tidak normal, kejadian yang jarang (*rare event*) atau kasus yang tidak biasa dalam sebuah dataset[1]. *Anomaly detection* sendiri memiliki pengaplikasian yang sangat luas, misalnya dalam diagnosis medis, pendeteksian penipuan komersian (*fraud)*, analisis pasar modal hingga pendeteksian penyusup pada jaringan. Telah banyak penelitian *anomaly detection* yang telah dilakukan termasuk penulis dalam mengaplikasikannya dalam sistem *access control* dalam *Integrated Smart Lock.*

Latar Belakang

Salah satu aspek keamanan yang paling penting dalam sistem keamanan gedung adalah sistem *access control* pada ruangan-ruangan penting. *Access control* sendiri adalah sebuah cara untuk membatasi akses terhadap sebuah sistem atau terhadap sumberdaya fisik maupun virtual, agar hanya orang tertentu saja yang memiliki akses terhadap sistem.

Smart Lock adalah perangkat penguncian elektronik yang dirancang untuk melakukan penguncian dan membuka kunci pada pintu dengan autentikasi dari pengguna yang memiliki akses. Sampai saat ini, banyak gedung-gedung seperti kampus yang masih mengaplikasikan sistem keamanan pada ruangan-ruangannya dengan menggunakan kunci tradisional. Hal ini tentu memiliki banyak kekurangan, misalnya mudah untuk diduplikat, rawan hilang maupun rusak.

Sebagai solusi dari permasalahan diatas, dibutuhkan sebuah sistem keamanan, khususnya pada ruangan-ruangan yang ada pada gedung yang terintegrasi dalam sebuah sistem. Salah satu solusi yang dapat diterapkan adalah dengan menggabungkan konsep dari *access control* dan *smart lock* menjadi sebuah *Integrated Smart Lock*. Dengan konsep ini, sistem bisa melakukan fungsi *controlling* dan *monitoring* untuk mengontrol dan memantau riwayat pengaksesan terhadap ruangan-ruangan yang ada.

Dalam pengimplementasian sistem ini, dibutuhkan sebuah cara untuk mengantisipasi ancaman yang bisa saja terjadi, seperti anomali, misalnya percobaan membuka pintu pada dinihari. Dalam menentukan metode machine learning yang tepat dalam melakukan pendeteksian anomali, kita harus melihat perbedaan dari metode yang ada. Metode *Supervised Learning* biasanya membuat sebuah model prediksi untuk anomaly berdasarkan data yang memiliki label (*training set*) dan menggunakannya untuk mengklasifikasikan tiap-tiap kejadian. Kekurangan utama dari metode ini adalah harus memiliki data yang memiliki label sehingga tidak mampu dalam mendeteksi kejadian baru dalam anomali. Sedangkan metode *Unsupervised Learning* pada umumnya tidak membutuhkan data berlabel karena dalam mendeteksi anomali metode ini menganggap data yang sangat berbeda dengan data 'normal' (mayoritas) sebagai anomali, sehingga kelebihannya adalah dapat beradaptasi dan mendeteksi kejadian anomali baru namun berpotensi mendapatkan nilai *false positive* yang tinggi[2].

Salah satu algoritma yang bisa digunakan untuk itu adalah algoritma *Kernel Density Estimation*. Konsep dasar dari KDE adalah mengestimasi fungsi densitas di suatu titik x dengan menggunakan pengamatan disekitaran[3].

Topik dan Batasannya

Berdasarkan latar belakang di atas, muncul beberapa masalah yang berhasil diidentifikasikan, yaitu bagaimana mengimplementasikan konsep *Smart Lock* dalam sistem *Integrated Smart Lock* dengan menggunakan metode *Unsupervised Learning* untuk mendeteksi terjadinya. Jenis metode *Unsupervised Learning* yang digunakan adalah *Kernel Density Estimation*. Input dari KDE yang digunakan dalam penelitian ini adalah berupa riwayat pengaksesan *smart lock* oleh pengguna sehingga didapatkan frekuensi dari pengaksesan pada jam-jam tertentu, sedangkan outputnya adalah berupa sebuah kurva *Probability Density Function* (PDF) yang nantinya akan digunakan untuk menghitung anomaly score. Dalam pengembangannya sistem ini akan diimplementasikan dan didukung oleh tiga buah sub-sistem/aplikasi, yaitu sistem *smart-lock* berbasis mikrokontroller, aplikasi web admin dan aplikasi android untuk pengguna.

Namun dalam penelitian ini, tentunya terdapat batasan-batasan dalam pengerjaannya, yaitu sistem yang dibuat terutama sistem *smart lock*-nya sendiri yang berupa alat-alat microcontroller, sensor dan aktuator seperti Arduino Uno, Ethernet Shield, RFID Reader RC-522, Relay, Solenoid dan Buzzer hanya berupa model *prototype* serta dalam implementasi *Kernel Density Estimation* hanya menggunakan satu fungsi kernel yaitu fungsi kernel *Gaussian*.

Tujuan

Berdasarkan perumusan masalah di atas, tujuan dari penulis dari penelitian ini adalah untuk membuat sebuah sistem *smart lock* yang terintegrasi yang dilengkapi dengan aplikasi web dan android yang menggunakan metode *Kernel Density Estimation* dalam pendeteksian anomaly dalam pengaksesan sistem *smart lock*-nya. Berikut merupakan poin-poin tujuan dalam penelitian ini :

Tabel 1 Keterkaitan antara tujuan, pengujian dan kesimpulan

No	Tujuan	Pengujian	Kesimpulan
1	Mengimplementasikan konsep *Smart Lock* dalam sistem *Integrated Smart Lock*.	Menguji rangkaian sistem yang terdiri dari aplikasi web dan android serta sistem *smart lock* yang menggunakan Arduino Uno, Ethernet Shield, RFID Reader RC-522, Relay, Solenoid dan Buzzer.	Prototipe alat siap untuk digunakan seusai fungsionalitas untuk dilakukan uji coba.
2	Menerapkan metode *Kernel Density Estimation* untuk mendeteksi anomali.	Menguji metode *Kernel Density Estimation* dengan kernel Gaussian dalam pendeteksian anomali saat pengaksesan smart lock.	*Kernel Density Estimation* mampu menampilkan *Probability Density Function* yang digunakan untuk menghitung *anomaly score.*
3	Menghasilkan sebuah metode *anomaly detection* yang efektif dalam mendeteksi terjadinya anomali.	Menguji tingkat akurasi serta menghitung FAR dan FRR dari metode *anomaly detection* yang digunakan	Metode *Anomaly Detection* menghasilkan efektif dalam melakukan pendeteksian anomali.