BAB 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan era digital yang pesat memungkinkan setiap organisasi dan individu untuk mengelola informasi dengan lebih cepat dan efektif. Seiring meningkatnya penggunaan aplikasi berbasis web dalam berbagai bidang, termasuk perusahaan, ancaman keamanan data menjadi isu yang mendesak, terutama dalam hal serangan siber yang menyasar data sensitif. Salah satu ancaman keamanan utama SQL Injection (SQLi), yaitu serangan yang memanfaatkan celah pada aplikasi untuk menyuntikkan kode SQL berbahaya yang dapat mengakses informasi sensitif yang disimpan di *server database*, seperti privasi pengguna dan data perusahaan[1]. Rata-rata, serangan web yang dilakukan dengan SQL Injection menyebabkan kerugian hingga $10 miliar pada ekonomi AS setiap tahunnya[2]. Menurut *Open Web Application Security Project* (OWASP), SQL Injection masih termasuk dalam top 10 besar risiko keamanan aplikasi web tahun 2021[3]. Berbagai metode deteksi dan pencegahan SQL Injection telah dikembangkan, namun para pelaku ancaman terus menyesuaikan strategi pencegahan yang ada. Secara teoritis, semua aplikasi web yang berjalan dengan database mungkin rentan terhadap serangan SQL Injection[4].

Penelitian sebelumnya, seperti yang dilakukan oleh Alan Paul dan rekan-rekannya pada tahun 2022, pada penelitian tersebut menggunakan 457.233 *dataset* dan menggunakan model *hybrid* CNN-LSTM untuk mendeteksi dan mengklasifikasikan serangan, mencapai tingkat akurasi yang tinggi dengan *F1-Score* rata-rata 97% dalam mendeteksi lalu lintas jaringan berbahaya[1]. Kombinasi CNN-LSTM dipilih karena CNN mampu mendeteksi pola teks yang kompleks tanpa menggunakan fitur yang rumit, sementara LSTM mengurangi kesalahan *false negative* pada data berurutan. Kombinasi kedua model tersebut diharapkan dapat meningkatkan akurasi dan kecepatan respons model CNN-LSTM, serta memberikan kemampuan deteksi SQL Injection yang lebih baik terhadap berbagai serangan yang muncul secara dinamis.

Metode deteksi dinamis dipilih untuk analisis keamanan aplikasi web karena memiliki keunggulan dalam mengidentifikasi pola serangan yang terus bervariasi dan berkembang. Deteksi statis yang bergantung pada pola serangan aturan tetap yang sudah dikenal, tidak dapat menemukan serangan baru atau varian dari ancaman yang sudah ada. Sedangkan, metode deteksi dinamis dapat menganalisis input atau *traffic* secara langsung, memungkinkan untuk mengidentifikasi serangan SQL Injection yang tidak terdeteksi metode statis. Dengan menggunakan deteksi dinamis berbasis model *deep learning* akan meningkatkan kemampuan sistem untuk mendeteksi pola serangan SQL Injection yang muncul secara *real-time*.

Model CNN-LSTM yang telah dievaluasi diintegrasikan ke dalam aplikasi web menggunakan *framework* Flask, memungkinkan deteksi serangan SQL Injection secara *real-time* dan meningkatkan keamanan web[5]. Flask memungkinkan pembuatan API yang dapat menerima masukan dari pengguna, memprosesnya dengan model CNN-LSTM, serta mengembalikan prediksi keamanan[5]. Flask dibuat menggunakan Python, sehingga mendukung integrasi langsung dengan model *deep learning* untuk mendeteksi pola serangan SQL Injection. Flask memiliki keunggulan untuk menerima dan mengirim data dalam format JSON, yang dapat langsung diolah langsung oleh model *deep learning*. Kombinasi keunggulan pengelolaan *deep learning* oleh Flask dan keamanan Laravel 10 pada aplikasi web memungkinkan deteksi serangan yang cepat dan dinamis tanpa perlu mengorbankan performa dan keamanan aplikasi.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan model deteksi SQL Injection berbasis deep learning dengan kombinasi *Convolutional Neural Network* (CNN) dan *Long Short-Term Memory* (LSTM), yang diintegrasikan secara dinamis melalui API Flask pada aplikasi web Laravel 10. Model *deep learning* dirancang untuk memberikan solusi yang fleksibel dalam menghadapi ancaman SQL Injection yang terus berkembang. Diharapkan dalam sistem ini dapat mendeteksi ancaman secara *real-time*, akurasi tinggi, dan mengurangi dampak resiko kebocoran data dengan memanfaatkan kemampuan CNN untuk mendeteksi pola teks yang kompleks dan LSTM untuk mengurangi negatif palsu. Keberhasilan model ini akan memberikan kontribusi signifikan dalam

memperkuat keamanan aplikasi web dan melindungi data sensitif dari serangan siber.

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, serangan SQL Injection masih menjadi ancaman serius bagi aplikasi web, maka dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana mengembangkan deteksi SQL Injection berbasis *deep learning* terhadap serangan SQL Injection dengan kombinasi CNN-LSTM untuk meningkatkan akurasi dan kecepatan respons?
2. Bagaimana model CNN-LSTM yang diintegrasikan dengan API Flask dapat diterapkan pada aplikasi berbasis Laravel untuk mendeteksi SQL Injection secara dinamis?

1.3. Tujuan dan Manfaat

Tujuan utama dari penelitian ini yaitu dengan rincian sebagai berikut:

1. Mengembangkan model deteksi SQL Injection berbasis *deep learning* yang memiliki akurasi dan kecepatan respons model CNN-LSTM dalam mendeteksi pola serangan SQL Injection.
2. Mengintegrasikan model CNN-LSTM dengan API Flask pada aplikasi berbasis Laravel 10 untuk mendeteksi serangan SQL Injection secara dinamis.

1.4. Batasan Masalah

Adapun batasan masalah adalah sebagai berikut:

1. Dataset yang digunakan bersumber dari platform Kaggle yang dipublikasikan oleh Gambler Yu, yaitu *Dataset Biggest* SQL Injection 2022.
2. Fokus deteksi SQL Injection pada aplikasi web berbasis Laravel, tanpa mencakup jenis serangan lainnya.

1.5. Hipotesis

Hipotesis penelitian ini adalah untuk mengembangkan model deteksi SQL Injection dengan berbasis *deep learning* menggunakan model CNN-LSTM yang

mampu mendeteksi serangan SQL Injection secara akurat dan respons yang cepat. Model CNN-LSTM yang diusulkan akan memberikan kinerja deteksi yang lebih baik dibandingkan dengan model tradisional dari akurasi dan kecepatan respons. Selain itu, model CNN-LSTM yang diimplementasikan dengan API Flask pada aplikasi Laravel, yang memungkinkan deteksi secara dinamis pada aplikasi web. Integrasi ini meningkatkan efisiensi dalam mendeteksi SQL Injection, dengan memanfaatkan API Flask sebagai penghubung antara model *deep learning* dengan aplikasi web Laravel.

Penelitian yang dilakukan oleh Tae-Yong Kim menunjukkan bahwa model CNN-LSTM mencapai performa *accuracy* 93.77% dan *F1-Score* mencapai 92.91%[6]. Penelitian tersebut juga membandingkan metode deteksi SQL Injection menggunakan model *deep learning* lainya seperti DNN, LSTM, CNN, LSTM+DNN, CNN+DNN. Namun, deteksi menggunakan *hybrid* CNN-LSTM memiliki keunggulan jauh lebih baik dibandingkan algoritma *deep learning* lainnya. Sehingga, perkiraan hasil penelitian ini menyamai atau meningkat dari akurasi model *deep learning* dalam mendeteksi SQL Injection. Jika hipotesis penelitian ini terbukti benar. Maka, model *deep learning* CNN-LSTM menjadi solusi yang baik untuk deteksi SQL Injection secara dinamis untuk meningkatkan keamanan pada aplikasi web.

1.6. Jadwal Pelaksanaan

Kegiatan dimulai dengan kajian pustaka untuk memahami konsep dan metode deteksi SQL Injection secara mendalam berbasis *deep learning* dengan model CNN-LSTM. Kajian pustaka diambil dari sumber informasi yang dapat diakses melalui seperti *Scopus*, *ScienceDirect* dan sumber lainnya. Jurnal yang digunakan dalam kajian pustaka mencakup dari tahun 2020 hingga 2024. Pada tahap ini, fokus diberikan pada pemahaman mengenai manfaat CNN dan LSTM dalam mengidentifikasi pola serangan yang kompleks pada *dataset* berlabel SQL Injection. Langkah berikutnya adalah pengumpulan *dataset* secara kuantitatif, dengan mengakses dataset SQL Injection melalui platform Kaggle. *Dataset* yang yang dipilih adalah dataset yang sudah memiliki label untuk memudahkan dapat mengklasifikasikan *query* berbahaya dan tidak berbahaya. *Dataset* kemudian

dilakukan data *preprocessing* dan *feature extraction* untuk memudahkan model *deep learning* mengolah *dataset*.

Rancangan penelitian selanjutnya adalah membangun model *deep learning* CNN-LSTM dari *dataset*. Model CNN-LSTM disusun dalam beberapa lapisan secara sistematis untuk menghasilkan representasi yang mendalam dari data input, sehingga dapat mengenali pola serangan SQL Injection dengan akurasi tinggi. Setelah model selesai dilatih, selanjutnya dilakukan evaluasi *accuracy*, *precision*, *recall* dan *F1-Score*. Evaluasi ini penting untuk menilai kemampuan model dalam mendeteksi SQL Injection. Ketika model sudah mencapai akurasi yang memadai, dilanjutkan dengan tahap integrasi dengan aplikasi web Laravel 10 melalui API Flask. Tujuan integrasi adalah untuk memungkinkan deteksi serangan SQL Injection dilakukan secara otomatis dan dinamis setiap kali dimasukan ke dalam aplikasi.

Tahap akhir dari model yang sudah diintegrasikan akan diuji dalam skenario serangan untuk mengukur tingkat akurasi mengenali berbagai pola SQL Injection, serta kecepatan respons dalam mendeteksi serangan di lingkungan pengujian. Keseluruhan proses dalam kegiatan ini dirangkum dalam laporan akhir, yang mencakup kesimpulan hasil dan saran untuk langkah langkah tambahan.

Tabel 1.1 Jadwal Kegiatan

Kegiatan	**Bulan**					
	1	2	3	4	5	6
Melakukan kajian pustaka.						
Pengumpulan *dataset* SQL Injection melalui platform kaggle untuk model.						
Pengembangan model CNN-LSTM dengan *dataset* dan evaluasi akurasi model.						
Melakukan Integrasi model deep learning dengan API Flask dan aplikasi web Laravel 10.						
Pengujian terhadap model CNN-LSTM terhadap SQL Injection secara dinamis.						
Penyusunan laporan akhir dan kesimpulan.						