BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi adalah upaya melindungi data dan sistem dari akses, penggunaan, atau perubahan yang tidak sah, sehingga menjaga kerahasiaan, integritas, dan ketersediaan informasi. Penggunaan basis data adalah proses penyimpanan, pengelolaan, dan pengaksesan data secara terstruktur untuk mendukung pengambilan keputusan dengan lebih efisien dan efektif. Structured Query Language (SQL) adalah bahasa populer yang digunakan untuk mengakses dan mengelola basis data. Namun, Structured Query Language (SQL) juga memiliki kelemahan yang dapat menjadi celah keamanan yang dikenal sebagai SQL Injection. Berdasarkan statistik yang diperoleh dari Open Worldwide Application Security Project (OWASP), SQL Injection (SQLI) merupakan ancaman besar bagi aplikasi web[1]. SQL Injection (SQLI) terjadi ketika penyerang menyisipkan kueri berbahaya ke dalam input yang tidak sah pada aplikasi web yang memungkinkan eksekusi langsung ke dalam basis data. Bahayanya, jika SQL Injection (SQLI) tidak diatasi, mengakibatkan penyerang dapat mengambil alih dan merusak basis data, mencuri data sensitif, mengubah maupun menghapusnya.

Deteksi SQL Injection (SQLI) memiliki dua pendekatan, di mana pada pendekatan pertama, *source code* digunakan untuk memvalidasi input pengguna, sementara pada pendekatan kedua, kueri dijalankan melalui perangkat lunak tambahan yang melewati aplikasi web untuk diverifikasi. Pendeteksian dari kedua pendekatan tersebut telah dipelajari menggunakan berbagai teknik dengan kelebihan dan kelemahan masing-masing. Pada penelitian pertama ini Candidate Evaluation for Discovering Intent Dynamically (CANDID) [2] digunakan untuk mengatasi keterbatasan sistem yang sebelumnya diusulkan dengan menggunakan basis data yang berbeda dan dengan membedakan struktur untuk mendeteksi SQL Injection (SQLI). Pada penelitian kedua Penggabungan pendekatan Statis dan

Dinamis digabungkan dalam sebuah alat yang bernama "amnesia" yang digunakan untuk mendeteksi SQL Injection (SQLI)[3]. Teknik tradisional hanya efektif dalam mendeteksi sedikit jumlah kueri berbahaya dan gagal mendeteksi kueri baru yang dikembangkan oleh para peretas. Penggunaan *machine learning* dalam mendeteksi SQL Injection (SQLI) telah memungkinkan pendeteksian kueri berbahaya yang baru dikembangkan oleh para peretas serta membantu meningkatkan sistem deteksi SQL Injection (SQLI) saat ini dengan efektifitas yang lebih baik dari pada teknik tradisional. Zhang [4] mengusulkan melakukan analisis perbandingan pada berbagai klasifikasi menggunakan Bag-Of-Words (BOW), Inverted Sentence Vector (IVS), dan *word2vec* sebagai fitur untuk mendeteksi SQL injection (SQLI). Uwagbole [5] menggunakan Support Vector Machine(SVM) untuk mendeteksi SQL injection, metode ini terbukti efektif dalam memblokir permintaan web berbahaya untuk memanipulasi *database backend* guna manipulasi data menggunakan SQL injection(SQLI). Kindy [6] melakukan perbandingan terhadap berbagai jenis algoritma untuk SQL Injection(SQLI) dalam bahasa pemrograman *PHP*. Hasil menunjukkan bahwa Convolutional Neural Network(CNN) dan Multi Layer Preceptron (MLP) memiliki akurasi dan presisi yang lebih baik dibandingkan dengan algoritma pembelajaran mesin lainnya. Li [7] mengusulkan metode deteksi SQL Injection(SQLI) berbasis LSTM (Long Short-Term Memory) untuk mengembangkan sistem deteksi SQL Injection(SQLI) yang cerdas. Sistem ini terbukti efektif dalam mendeteksi SQL Injection(SQLI) yang kompleks dengan jumlah data yang besar dan rumit. Metode tradisional memiliki kelemahan dalam mendeteksi serangan baru maupun metode *machine learning* dan *deep learning* yang di usulkan peneliti dalam deteksi SQL Injection(SQLI) memiliki kelemahan dalam representasi fitur dan efisiensi algoritma, sehingga dengan mengusulkan metode *hybrid* yaitu algoritma Convolutional Neural Network-Long Short Term Memory(CNN-LSTM) dapat mengatasi kelemahan tersebut.

Metode hybrid yang diusulkan yaitu Convolutional Neural Network-Long

Short Term Memory (CNN-LSTM) memiliki keunggulan dalam memanfaatkan representasi fitur yang kuat dari Convolutional Neural Network (CNN), *model* dapat mengekstraksi informasi yang kaya dan mendalam dari data teks, termasuk teks yang terkait dengan serangan SQL Injection (SQLI). Selain itu, kemampuan Long Short Term Memory (LSTM) dalam memproses urutan kata dalam teks memungkinkan *model* untuk memahami konteks temporal dan dependensi antara kata-kata, yang membantu dalam mengenali pola urutan yang relevan untuk mendeteksi serangan SQL Injection (SQLI). Dengan kombinasi fitur ini, *model hybrid* ini dapat lebih baik dalam menggeneralisasi pada serangan baru dan memberikan hasil yang lebih baik dalam mendeteksi serangan SQL Injection (SQLI) dengan akurasi tinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, masalah pada teknik tradisional memiliki masalah dalam mendeteksi serangan baru, sedangkan pada *deep learning* dan *machine learning* yang menggunakan algoritma tunggal memiliki masalah pada representasi fitur dan efiensi algoritma yang lemah, Maka dapat disimpulkan poin pertanyaan penelitian sebagai berikut:

1. Bagaimana kinerja *model* Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) dalam mendeteksi adanya serangan SQL Injection(SQLI)?

1.3 Batasan Masalah

Untuk Batasan masalah dalam penelitian ini adalah:

1. Dalam penelitian ini menggunakan arsitektur satu dimensi Convolutional Neural Network(CNN) dan Long Short Term Memory (LSTM)
2. Dataset SQL Injection (SQLI) diambil dari Kaggle[8].

3. Penelitian ini hanya pada tahapan pemodelan data, dan belum sampai pada tahapan implementasi *model* ke sistem maupun aplikasi.
4. Pada bagian pengujian *model* atau sistem hanya menggunakan *kueri* injeksi tanpa menggunakan *kueri* normal.

1.4 Tujuan Penelitian

Berikut adalah tujuan dari penelitian ini adalah:

1. Melakukan eksperimen terhadap kombinasi *model* Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) serta mengetahui kinerja *model* tersebut dalam mendeteksi serangan SQL Injection(SQLI).

1.5 Manfaat Penelitian

Penelitian ini memiliki manfaat sebagai berikut:

1. Meningkatkan keamanan sistem: Dengan mengetahui kinerja *model* Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) dalam mendeteksi SQL Injection(SQLI), penelitian ini dapat membantu meningkatkan keamanan sistem yang rentan terhadap serangan SQL Injection(SQLI).

1.6 Sistematika Penulisan

Berikut adalah uraian singkat isi penulisan skripsi:

BAB I PENDAHULUAN, Latar belakang masalah berisi gambaran tentang masalah penelitian, Rumusan masalah berisi simpulan dan poin penting dari masalah yang ada pada latar belakang, Batasan masalah berisi variabel yang diteliti, Tujuan penelitian berisi hal yang akan dilakukan pada penelitian, manfaat penelitian berisi hasil tujuan penelitian , dan sistematika penulisan berisi uraian secara garis besar tiap bab.

BAB II TINJAUAN PUSTAKA, Studi literatur berisi rangkuman penelitian sebelumnya dalam lima tahun terakhir yang relevan dengan

topik, tabel keaslian penelitian berisi enam penelitian sebelumnya yang dibandingkan dengan punya peneliti, dan dasar-dasar teori berisi teori yang digunakan sesuai dengan topik.

BAB III METODE PENELITIAN, Alat dan bahan berisi tools dan dataset, serta alur penelitian berisi Langkah-langkah dalam melakukan penelitian.

BAB IV HASIL DAN PEMBAHASAN, Pemodelan berisi uraian penjelasan tahap dan hasil, serta pengujian berisi uraian tahap dan hasil.

BAB V PENUTUP, kesimpulan berisi kesimpulan dari rumusan masalah dan hasil yang diperoleh dan saran berisi kekurangan dari penelitian yang dapat dilakukan peneliti lain jika mengambil topik yang sesuai.