BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Serangan kejahatan siber memiliki banyak jenis serangan kejahatan yang harus diketahui. Keberagaman jenis serangan siber menunjukkan bahwa sistem digital menghadapi ancaman yang semakin kompleks dan memerlukan pendekatan keamanan yang komprehensif. Beberapa jenis serangan kejahatan siber yang paling umum yaitu *Malware (Malicious Software) , Phishing, Man-in-the-Middle (MitM), Ransomware, SQL Injection, Cross-Site Scripting (XSS), Social Engineering,* Kejahatan Identitas *(Identity Theft), dan IoT Exploitation* (Laksana, T. G., & Mulyani , S, 2024).

Serangan *SQL Injection* menjadi ancaman keamanan aplikasi web beberapa tahun terakhir. Tingginya serangan mengindikasikan bahwa mekanisme perlindungan aplikasi web yang masih memiliki kelemahan mendasar. Pada saat ini OWASP Foundation (2025) menyatakan bahwa *injection* menduduki peringkat ke-5 teratas OWASP Top 10 tahun 2025 dengan potensi menyebabkan kebocoran jutaan data sensitif melalui manipulasi kueri database yang tidak tervalidasi. Peringkat tersebut menunjukkan bahwa *SQL Injection* bukan hanya masalah teknis, namun juga resiko strategis terhadap keamanan data. Penyerang memanfaatkan input user yang tidak difilter untuk menyisipkan kode berbahaya, mengubah struktur kueri SQL asli, dan mengakses/menghapus data secara tidak sah.

Serangan *SQL Injection* dapat terjadi ketika penyerang yang memiliki pengetahuan tentang kueri SQL dapat melewati kelemahan keamanan dilapisan basis data aplikasi. Hal ini menunjukkan bahwa tingkat keahlian penyerangan berbanding lurus dengan tingkat risiko yang dihadapi sistem. Kerentanan ini terjadi ketika input dari pengguna tidak difilter dengan benar, terutama untuk karakter meta saat menggunakan formulir input. Kegagalan dalam validasi input tersebut secara langsung membuka celah manipulasi kueri SQL. Oleh sebab itu, serangan *SQL Injection* terus menjadi salah satu metode yang disukai para penyerang untuk mengakses dan mengubah data website (Jumaryadi dkk., 2024).

SQL Injection adalah teknik serangan siber yang sering digunakan untuk merusak atau mengakses data sensitif dalam sistem basis data. Efektivitas tinggi serangan ini menjadikannnya salah satu metode paling berbahaya dalam keamanan siber. Di antara berbagai teknik dalam keamanan siber, ini adalah salah satu teknik keamanan siber yang memiliki efektivitas yang tinggi dalam memanipulasi atau mencuri informasi melalui celah keamanan pada sistem. Penjahat siber menggunakan *SQL Injection* untuk mengancam keamanan aplikasi berbasis web. Memasukkan perintah SQL yang berbahaya kedalam input aplikasi untuk dieksekusi oleh aplikasi. Serangan ini menggunakan kerentanan yang terdapat dalam aplikasi yang tidak memvalidasi atau membersihkan input pengguna dengan baik, yang memungkinkan eretas untuk mengakses, mengubah atau menghancurkan data di basis data (Syarifah, 2024).

Pada penelitian (Rizkinaswara, 2020), *Internet of Things, Big Data, Artificial Intelligence, Cloud Computing, dan Additive Manufacturing* merupakan lima teknologi utama yang mendorong Revolusi Industri 4.0 untuk membangun industri siap digital. Di era digital yang semakin maju, *machine learning* dan *Artificial Intelegence* (AI) termasuk komponen penting dari keamanan siber (Harkin and Molnar 2023). Pemanfaatan AI memungkinkan sistem keamanan beralih dari pendekatan reaktif menjadi proaktif. Teknologi ini dapat membantu sistem keamanan siber mendeteksi dan mencegah serangan kejahatan siber. Penggunaan AI dan *machine learning* dapat digunakan untuk menemukan pola serangan yang tidak biasa dengan mempelajari perilaku biasa pengguna dan secara otomatis mengambil tindakan preventif (Barth dkk., 2020).

Deep Learning saat ini berperan sebagai pendekatan evaluasi yang menyeluruh dan meyakinkan terhadap sistem keamanan jaringan. Kemampuannya dalam memroses data kompleks menjadikan *Deep Learning* sebagai bagian integral dari keamanan jaringan. *Deep Learning* didefinisikan sebagai penggunaan jaringan saraf tiruan secara mendalam yang dihubungkan menggunakan beberapa lapisan untuk menghasilkan output. Agar dapat menghasilkan suatu luaran, hasil dari tahap sebelumnya digunakan sebagai input. Dengan berbagai keunggulannya dibandingkan dengan metode *Machine Learning* konvensional lainnya, algoritma

Deep Learning menjadi sangat penting dalam memecahkan masalah kompleks. Kemampuan *Deep Learning* dalam menghasilkan rekayasa fitur otomatis berkontribusi langsung terhadap peningkatan akurasi deteksi serangan, sehingga keamanan jaringan dapat ditingkatkan secara signifikan (Suartana, I. M., 2022).

Sebagai upaya deteksi serangan *SQL Injection*, penelitian ysng dilakukan oleh Pramono, N., & Sari, A. A. (2024), menerapkan algoritma *Support Vector Machine* (SVM) berbasis machine learning dengan tahapan praproses meliputi *case folding*, *stopword removal*, tokenisasi, serta ekstraksi fitur menggunakan TF-IDF. Akurasi tertinggi sebesar 96,84% pada rasio data latih dan data uji 70:30, yang menunjukkan bahwa SVM mampu menangani data teks secara efektif dan membentuk batas keputusan yang kuat.

Meskipun penelitian Ishak (2023) berhasil menunjukkan efektivitas algoritma machine learning dalam klasifikasi data teks, pendekatan yang digunakan masih bergantung pada ekstraksi fitur manual, sehingga berpotensi membatasi kemampuan model dalam menangkap pola lokal dan representasi semantik yang lebih kompleks. Selain itu, metode yang digunakan belum dirancang untuk menangani teks teknis dengan struktur khusus, seperti kueri SQL, yang memiliki karakteristik berbeda dibandingkan teks media sosial. Oleh karena itu, terdapat gap penelitian untuk menerapkan pendekatan *deep learning*, khususnya *Text Convolutional Neural Network* (TextCNN), yang mampu melakukan ekstraksi fitur secara otomatis, menangkap pola lokal dalam teks, serta memberikan kinerja yang lebih efisien dan akurat dalam mendeteksi pola berbahaya pada kueri SQL Injection berbasis aplikasi web.

Penelitian oleh Chen dkk., (2020) yang membahas teknik deteksi dan pencegahan serangan SQL Injection menggunakan pendekatan *Deep Learning*. Penelitian ini bertujuan untuk mengembangkan pendekatan ringan untuk mendeteksi dan mencegah serangan *SQL Injection* dengan memanfaatkan embedding kata dan algoritma *Deep Learning* dengan CNN (*Convolutional Neural Network*) dan MLP (*Multi-Layer Perceptron*). Pendekatan ini menekankan pentingnya keseimbangan antara akurasi deteksi dan efisiensi sistem.

Berbagai metode deteksi *SQL Injection* telah dikembangkan dari machine learning seperti SVM, Random Forest, serta model *Deep Learning*. Namun, tingginya kompleksitas dan kebutuhan sumber daya besar menjadi kendala utama dalam penerapan sistem secara *real-time*. Text Convolutional Neural Network (TextCNN) muncul sebagai solusi yang relatif ringan dan efektif mendeteksi pola lokal dalam data teks seperti kueri SQL berbahaya, dengan kecepatan tinggi dan performa deteksi efektif. Karakteristik ini menjadikan TextCNN lebih sesuai untuk lingkungan aplikasi web yang memerlukan respon *real-time* dengan keterbatasan sumber daya.

Penelitian ini berfokus pada penerapan algoritma TextCNN yang mampu memberikan keseimbangan antara tingkat akurasi yang baik dan efisiensi komputasi. Penelitian ini dibatasi pada pengembangan sistem deteksi SQL Injection berbasis TextCNN dengan menggunakan data kueri teks pada aplikasi web. Selain itu, penelitian hanya mencakup deteksi serangan first-order SQL Injection agar fokus penelitian lebih jelas dan terukur. Pengujian sistem dilakukan dalam lingkungan simulasi web, sehingga hasil penelitian masih memerlukan pengujian lanjutan pada lingkungan produksi yang sebenarnya.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah diuraikan, telah ditemukan rumusan masalah yang diidentifikasi diantaranya berikut :

1. Bagaimana mengembangkan sistem deteksi SQL Injection berbasis aplikasi web menggunakan algoritma TextCNN?
2. Bagaimana performa sistem deteksi dalam melakukan deteksi *SQL Injection*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan dalam penelitian ini ialah sebagai berikut:

1. Mengembangkan sistem deteksi *SQL Injection* menggunakan sistem deteksi berbasis aplikasi web menggunakan algoritma TextCNN.

2. Menguji performa sistem deteksi *SQL Injection* berbasis website melalui pengujian blackbox dan metrik evaluasi.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan keilmuan dibidang pengembangan keamanan jaringan, terutama melalui pemanfaatan konsep ilmu komputer untuk membangun aplikasi web yang mampu mendeteksi seranagn *SQL Injection* menggunakan algoritma TextCNN .Penelitian ini juga bertujuan untuk memperdalam pemahaman mengenai terkait mekanisme kerja model TextCNN dalam mengenali pola-pola serangan *SQL Injection* pada data berbentuk teks.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan manfaat praktis dari penelitian ini yaitu:

1. Bagi pengembang aplikasi, sistem ini dapat menjadi landasan dalam pengembang aplikasi web untuk mengintegrasikan fitur deteksi serangan yang cepat dan akurat menggunakan TextCNN, juga membantu mengurangi risiko kebocoran data dan meningkatkan keamanan aplikasi berbasis web secara berkelanjutan.
2. Bagi peneliti, penelitian ini dapat berfungsi sebagai referensi dalam kajian lanjutan mengenai penerapan algoritma TextCNN untuk deteksi serangan *SQL Injection*. Selain itu, temuan penelitian ini juga dapat menjadi acuan dalam menyelesaikan permasalahan serupa yang berkaitan dengan keamanan aplikasi berbasis web

1.5 Ruang Lingkup Penelitian

Penelitian ini berfokus pada implementasi algoritma TextCNN dalam sistem deteksi serangan *SQL Injection* berbasis aplikasi web. Ruang lingkup penelitian meliputi:

1. Fokus penelitian adalah mendeteksi dan mengklasifikasikan kueri SQL sebagai aman atau mengandung serangan *SQL Injection*.
2. Dataset yang digunakan berupa kumpulan kueri SQL yang terdiri dari dua kelas, yaitu kueri normal (aman) dan kueri berbahaya (SQL Injection).
3. Penelitian ini menghasilkan sistem deteksi berbasis aplikasi web yang dapat mengenali dan mengklasifikasikan input pengguna dengan label "aman" atau "berbahaya".
4. Sistem deteksi hanya berfokus pada kueri SQL berbasis teks, dengan preprocessing meliputi tokenisasi dan padding, serta pemrosesan menggunakan model TextCNN.

1.6 Struktur Organisasi Skripsi

Dalam penulisan sistematika pada penyusunan laporan penelitian ditulis menurut Pedoman Penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun 2024, terdapat urutan rangkaian yang membahas setiap bab tersebut diantaranya :

1. PENDAHULUAN

   Bagian Bab I ini Memberi penjelasan secara sistematis terkait latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan struktur organisasi penulisan skripsi.
2. TINJAUAN PUSTAKA

   Menguraikan hasil tinjauan dari teori penelitian yaitu mengenai serangan SQL Injection, algoritma TextCNN, juga aplikasi deteksi berbasis web. Terdapat juga hasil-hasil penelitian yang relevan guna membantu dalam menyelesaikan permasalahan penelitian.
3. METODE PENELITIAN

   Menjelaskan tahapan-tahapan penelitian, objek penelitian dan metode penelitian yang akan digunakan, serta cara pengambilan dan cara mengolah data.
4. HASIL DAN PEMBAHASAN

   Menjelaskan hasil dari penelitian secara detail dan implementasi aplikasi web yang dibuat untuk mendeteksi serangan SQL Injection yang telah dibuat serta pengujian dan evaluasi terhadap kesesuaian penggunaan sistem.

5. SIMPULAN DAN SARAN

   Bab terakhir, yaitu simpulan dan saran, yang berisikan tafsiran dari hasil peneliian sebagai jawaban dari rumusan masalah penelitian sekaligus memberikan saran atau rekomendasi berdasarkan hasil dari penenelitian yang diberikan oleh peneliti.