BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Sebuah sistem terdiri dari beberapa komponen atau subsistem yang saling berinteraksi untuk mencapai sebuah tujuan. Dalam konteks organisasi, sistem ini mencakup berbagai elemen seperti individu, komputer, teknologi informasi, dan proses kerja. Sistem ini berfungsi untuk mengolah data menjadi informasi yang diperlukan untuk mencapai tujuan dan target yang telah ditetapkan (Sutabri et al., 2024).

Sebagai bagian integral dari revolusi digital, teknologi informasi telah mengalami pertumbuhan dan perkembangan yang signifikan dalam beberapa dekade terakhir. Salah satu aplikasi yang cukup menonjol dari teknologi ini adalah aplikasi berbasis *web*. Aplikasi berbasis *web* memiliki keunggulan dalam hal aksesibilitas, karena mereka dapat diakses dari lokasi mana pun dan kapan saja, selama ada koneksi internet dan perangkat lunak *browser web* yang tersedia tanpa harus melakukan instalasi (Yuningsih and Utami, 2024).

Meski aplikasi berbasis *web* memiliki keunggulan dalam hal aksesibilitas, namun mereka juga menghadapi beberapa ancaman kejahatan *cyber*. Salah satunya adalah *webshell*, yang merupakan ancaman keamanan serius pada aplikasi berbasis *web (Hartono and Khotimah, 2022)*. *webshell* adalah skrip yang dapat di

eksekusi oleh *server web* dan memberikan hak pengguna yang memiliki akses ke *server* tersebut. Contohnya adalah *PHP shell*, yang merupakan suatu bentuk implementasi *shell* berbasis *web*. Sebuah PHP *shell* yang berhasil diunggah memungkinkan penyerang untuk mengambil kendali atas *system* atau melakukan tindakan berbahaya sehingga menghasilkan serangan *webshell* atau eksekusi jarak jauh (Putra, 2023).

webshell biasanya digunakan oleh pihak tidak bertanggung jawab untuk mendapatkan kontrol penuh atas *server* yang terinfeksi. Deteksi w*ebshell* menjadi sebuah tantangan besar karena pola yang kompleks dan dinamis dari perilaku yang dilakukan oleh *webshell (Tianmin et al., 2019)*. Dalam penelitian ini, digunakan pendekatan *deep learing* untuk mendeteksi *webshell* terutama pada *server* aplikasi web ISB Atma Luhur.

ISB Atma Luhur juga sedang melakukan proses migrasi dari aplikasi berbasis desktop menjadi aplikasi berbasis *web*. Proses ini menimbulkan tantangan baru dalam hal keamanan, termasuk ancaman dari *webshell*. Selain itu, marak nya beberapa kasus aplikasi *web* lain yang telah menjadi target retasan dan penyebaran iklan judi *online* melalui aplikasi berbasis *web* pada *website* pemerintahan maupun akademik, menunjukkan betapa pentingnya peningkatan keamanan dalam aplikasi berbasis *web (Liputan6.com, 2024)*.

Tujuan utama penelitian ini adalah untuk mengembangkan model *deep learning* yang dapat mendeteksi *webshell* dengan tingkat presisi yang tinggi. *Deep*

learning dipilih berdasarkan penelitian terdahulu tentang perbandingan tradisional *machine learning* dan *deep learning* untuk teks klasifikasi (Kamath et al., 2018; Zulqarnain et al., 2020) . Model ini akan dilatih dengan menggunakan *dataset* berkas PHP yang telah di label, di mana label "*malicious*" menunjukkan adanya *webshell* dan label "*benign*" menunjukan tidak adanya *webshell*.

Untuk studi ini, model yang akan di gunakan dan di evaluasi adalah *Convolutional Neural Networks* (CNN) dan *Recurrent Neural Networks* (RNN) dengan *Long Short-Term Memory* (LSTM). Pada penelitian sebelumnya menunjukkan bahwa model LSTM dapat mencapai tingkat akurasi yang signifikan dalam teks klasifikasi (Sari et al., 2020; Semberecki and Maciejewski, 2017). Sama halnya dengan CNN yang juga yang terbukti efektif untuk klasifikasi teks (Semberecki and Maciejewski, 2017). Dengan mengintergrasikan kedua pendekatan ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam tentang penerapannya.

Penelitian ini akan berfokus pada model CNN dengan LSTM untuk klasifikasi *webshell* pada aplikasi berbasis web pada ISB Atma Luhur. Pendekatan ini penting dilakukan untuk mengidentifikasi kekuatan relatif masing-masing model dalam klasifikasi *webshell* (Putri et al., 2024). Dengan mengevaluasi kinerjanya, diharapkan dapat mengungkap baik kelebihan maupun kekurangan masing-masing model, serta strategi optimasi potensial untuk meningkatkan efektivitasnya dalam tugas klasifikasi teks yang kompleks

Penelitian ini penting karena dapat membantu untuk memperkuat keamanan *server* aplikasi *web* ISB Atma Luhur. Melalui deteksi *webshell*, ISB Atma Luhur dapat mencegah dan melindungi data sensitif yang disimpan pada *server* aplikasi *web*. Hasil dari penelitian ini diharapkan dapat digunakan sebagai alat untuk melindungi *server* aplikasi *web* ISB Atma Luhur dari ancaman keamanan *cyber.*

1.2 Rumusan Masalah Penelitian

Sesuai dengan uraian pada latar belakang masalah di atas, berikut adalah rumusan masalah yang dapat di buat:

a) Bagaimana cara efektif mendeteksi *webshell* pada *server* aplikasi web ISB Atma Luhur menggunakan pendekatan *deep learning*.

b) Bagaimana cara mencegah dan melindungi data sensitif yang disimpan pada *sever* aplikasi *web* ISB Atma Luhur dari ancaman keamanan *cyber.*

1.3 Batasan Masalah Penelitian

Berikut adalah batasan masalah yang ditetapkan untuk memperjelas topik yang akan dibahas dan menghindari pembahasan yang terlalu luas atau menyimpang:

a) Penelitian ini hanya fokus pada deteksi *webshell* pada *server* aplikasi *web* ISB Atma Luhur menggunakan pendekatan *deep learning* dan tidak mencakup deteksi *webshell* pada platform lain.

b) Model *deep learing* yang dikembangkan hanya dilatih dengan menggunakan *dataset* berkas PHP yang telah di label. Tidak mencakup dataset lain seperti *JavaScript* atau HTML.

c) Penelitian ini tidak mencakup peningkatan keamanan lainnya selain deteksi *webshell*. Misalnya, peningkatan keamanan *database*, *enkripsi* data, dan lain sebagainya.

d) Penelitian ini tidak mencakup penelitian bagaimana *webshell* bisa masuk ke *server*. Misalnya, bagaimana cara penyerang mengunggah *webshell* ke server, bagaimana cara penyerang mengakses server, dan lain sebagainya.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengembangkan model *deep learning* yang dapat mendeteksi *webshell* dengan tingkat presisi yang tinggi. Model ini akan dilatih dengan menggunakan *dataset* berkas PHP yang telah di label. Penelitian ini juga bertujuan untuk memperkuat *server* aplikasi web ISB Atma Luhur dan melindungi data sensitif yang disimpan pada *server* tersebut.

1.5 Manfaat Penelitian

Berikut adalah manfaat dari penelitian deteksi *webshell* dengan pendekatan *Deep Learning*.

a) **Peningkatan Keamanan:** Deteksi *webshell* secara otomatis dapat membantu dalam meningkatkan keamanan server. Dengan menggunakan teknologi *deep learing*, diharapkan model ini dapat mendeteksi aktivitas mencurigakan dan mengidentifikasi potensi ancaman seperti *webshell*.

b) **Efisiensi Waktu:** Proses deteksi manual dapat memakan waktu yang lama dan memerlukan pengetahuan khusus. Sebaliknya, dengan menggunakan model *deep learing*, diharapkan proses deteksi data dilakukan secara otomatis.

c) **Reduksi Biaya:** Dengan mengurangi resiko serangan dan kerugian yang mungkin ditimbulkan akibat serangan.

d) **Kontribusi Ilmiah:** Selain manfaat praktis nya, penelitian ini juga memberikan kontribusi ilmiah dalam bidang *cyber security*, khususnya dalam penggunaan *deep learing* untuk deteksi *webshell*. Hasil penelitian ini dapat digunakan sebagai referensi untuk penelitian-penelitian selanjutnya.

1.6 Ruang Lingkup Penelitian

Berikut adalah Ruang lingkup penelitian:

a) **Pengumpulan Data:** Pertama, peneliti akan mengumpulkan data berupa berkas PHP yang berupa *shell* dari Github, dan berkas PHP dari *framework* dan *cms* yang digunakan oleh ISB Atma Luhur. Setelah proses pengumpulan data selesai, peneliti akan memberikan label "0" untuk *webshell* dan "1" untuk berkas PHP yang telah diambil dari *framework* dan *cms* yang digunakan sebelumnya.

b) **Pembuatan Model Deep Learning:** Setelah data dikumpulkan, peneliti akan membuat model *deep learning*. Model ini akan dilatih dengan menggunakan *dataset* yang telah dikumpulkan. Tujuannya adalah untuk mampu mengenali apakah suatu berkas PHP adalah *webshell* atau bukan.

c) **Validasi Model:** Setelah model dibuat, peneliti akan melakukan validasi model. Validasi ini digunakan untuk memastikan bahwa model dapat mengenali *webshell* dengan presisi yang tinggi.

d) **Implementasi Model:** Jika model validasi memenuhi standar yang ditetapkan, maka model ini akan diimplementasikan pada aplikasi web di ISB Atma Luhur. Implementasi ini dilakukan untuk mendeteksi *webshell*.

e) **Evaluasi:** Setelah model diimplementasikan, peneliti akan melakukan evaluasi model. Evaluasi ini dilakukan untuk memastikan bahwa model

masih dapat mengenali *webshell* dengan presisi yang tinggi setelah di implementasi kan.

1.7 Susunan Dan Struktur Tesis

Struktur dan susunan penelitian tesis ini akan dibagi menjadi beberapa bab, yang akan dijelaskan sebagai berikut::

BAB I PENDAHULUAN

Bab ini mencakup: (a) Latar belakang masalah yang akan diteliti; (b) Rumusan permasalahan; (c) Tujuan penelitian, yang mencakup tujuan umum serta tujuan khusus yang terukur; (d) Harapan dan manfaat yang diharapkan dari hasil penelitian/analisis; (e) Ruang lingkup bahasan, termasuk area, substansi, wilayah geografis/topologi/administrasi, pendekatan penelitian, subjek, serta level pembahasan (makro atau mikro); dan (f) Susunan atau struktur tesis

BAB II KAJIAN PUSTAKA

Bab ini berisi kumpulan pustaka, kajian pustaka, dan/atau tinjauan literatur. Di dalam bab ini, dibahas berbagai publikasi resmi yang relevan dengan masalah yang diteliti atau model yang direncanakan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan secara rinci mengenai metodologi penelitian.

BAB IV HASIL PENELITIAN

Bab ini menyajikan hasil penelitian, termasuk gambaran mengenai objek yang diteliti..

BAB V PENUTUP

Bab ini menyajikan kesimpulan dari hasil penelitian secara sistematis, terkait dengan upaya untuk menjawab hipotesis dan/atau tujuan penelitian.

DAFTAR PUSTAKA

LAMPIRAN