BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang pesat telah membawa kemudahan dalam berbagai aspek kehidupan, termasuk dalam pertukaran data dan komunikasi. Namun, kemajuan ini juga dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan kejahatan siber. Salah satu metode yang sering digunakan adalah penyebaran URL berbahaya, yaitu tautan yang dirancang untuk mengelabui pengguna agar mengakses situs berbahaya yang dapat mencuri data pribadi atau menginfeksi perangkat dengan *malware*.

Menurut Rafi (2023), serangan umumnya melibatkan teknik *phishing* dan rekayasa sosial, dimana pelaku membuat domain yang menyerupai situs resmi. Pengguna yang kurang waspada dapat diarahkan ke situs palsu yang tidak hanya mencuri informasi sensitif seperti kredensial akun media sosial atau perbankan, tetapi juga menyebarkan *malware* ke seluruh jaringan perangkat korban. Dampak dari serangan ini sangat merugikan, mulai dari kerusakan sistem hingga hilangnya data penting yang sulit dipulihkan.

Upaya pencegahan tradisional, seperti pelatihan kesadaran keamanan siber, pemblokiran pop-up, dan penggunaan perangkat lunak antivirus, telah diterapkan untuk mengurangi risiko serangan. Namun, pendekatan ini bersifat reaktif dan memerlukan intervensi manual, sehingga kurang efektif dalam menghadapi serangan yang semakin kompleks dan dinamis. Selain itu, banyak perangkat lunak keamanan yang tidak mampu mendeteksi URL berbahaya baru tanpa pembaruan yang terus-menerus.

Seiring dengan perkembangan teknologi kecerdasan buatan, pendekatan berbasis machine learning telah digunakan untuk meningkatkan deteksi ancaman siber. Namun, banyak model yang masih memiliki keterbatasan dalam mengenali pola teks yang kompleks dan konteks yang berubah-ubah.

Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan integrasi Large Language Model (LLM) berbasis BERT ke dalam sistem Security Information and Event Management (SIEM). LLM memiliki kemampuan dalam memahami dan menganalisis pola bahasa alami secara mendalam, sehingga dapat meningkatkan akurasi dalam mendeteksi URL berbahaya secara otomatis dan real-time. Dalam implementasinya, dataset yang terdiri dari URL aman dan berbahaya akan digunakan untuk melatih model BERT. Model yang telah dilatih kemudian diintegrasikan ke dalam sistem SIEM, yang memungkinkan deteksi dini terhadap akses ke URL berbahaya dan memberikan respons aktif untuk mencegah potensi serangan.

Penelitian ini menggunakan SIEM berbasis Wazuh, yang dikenal dapat memantau keamanan, mendeteksi ancaman, dan menanggapi insiden secara real-time. Wazuh merupakan SIEM berbasis *open-source* yang memungkinkan pengguna untuk mengembangkan sistem sesuai dengan kebutuhan yang diperlukan, sehingga pengembangan pada penelitian ini menjadi optimal.

Dengan pendekatan ini, sistem keamanan siber diharapkan dapat beroperasi secara proaktif dan adaptif terhadap ancaman yang terus berkembang. Tujuan dari penelitian ini adalah merancang dan mengimplementasikan SIEM berbasis BERT yang mampu mendeteksi dan memblokir URL berbahaya dengan akurasi tinggi dan respons yang cepat, sehingga meningkatkan perlindungan terhadap ancaman siber yang semakin kompleks.

1.2 Identifikasi Masalah

Meningkatnya jumlah serangan siber di era digital menjadi ancaman serius bagi keamanan data pengguna. Salah satu metode serangan yang paling umum adalah melalui URL berbahaya, yaitu tautan yang secara sengaja dibuat untuk mengarahkan pengguna ke situs berbahaya. Situs ini dapat digunakan untuk mencuri informasi pribadi, menginfeksi perangkat dengan *malware*, hingga mengakses sistem tanpa izin. Untuk itu, dibutuhkan pendekatan yang lebih adaptif dan cerdas melalui pemanfaatan teknologi kecerdasan buatan, khususnya Large Language Model (LLM) berbasis BERT. Integrasi BERT ke dalam sistem S*ecurity Information and Event Management* (SIEM) diharapkan dapat menjadi solusi proaktif dalam mendeteksi dan mencegah akses ke URL berbahaya secara otomatis dan real-time.

1.2.1 Rumusan masalah

Berdasarkan identifikasi masalah yang ditemukan, penelitian ini merumuskan masalah yaitu, "Bagaimana mengembangkan *Security Information & Event Management (*SIEM*)* dengan Large Language Model berbasis BERT untuk mendeteksi, memprediksi dan mencegah akses pada URL berbahaya?"

1.2.2 Batasan masalah

Batasan masalah pada penelitian ini:

a) Data URL berbahaya yang digunakan dalam pengujian pada *Security Information & Event Management (*SIEM*)* harus diperbarui secara berkala, seiring terus bermunculannya URL berbahaya yang belum diketahui.
b) *Security Information & Event Management (*SIEM*)* ini tidak bertujuan untuk menggantikan solusi keamanan yang sudah ada, tetapi sebagai tambahan lapisan keamanan tambahan untuk pengguna internet dalam lingkup jaringan lokal.

1.3 Tujuan Penelitian

Membangun dan mengimplementasikan layanan deteksi URL berbahaya menggunakan Large Language Model (LLM) berbasis BERT, mengintegrasikan seluruh sistem deteksi dan pemblokiran dengan Wazuh SIEM untuk monitoring, *alerting*, pelaporan insiden keamanan, meminimalisir potensi akses pada *phishing*, *malware*, dan ancaman berbasis URL lainnya serta menyediakan *alert log* terpusat pada SIEM untuk analisis dan mitigasi insiden.

1.4 Manfaat Penelitian

Penelitian ini memiliki manfaat bagi tiga pihak: masyarakat, peneliti, dan ilmu pengetahuan. Berikut adalah rangkuman dan penjelasan manfaat tersebut.

a) Manfaat bagi Masyarakat

Solusi otomatis yang tersedia untuk memperkuat keamanan jaringan lokal—terutama di pemerintahan, sekolah, dan usaha kecil menengah—dengan memblokir URL berbahaya sebelum dapat diakses pengguna merupakan manfaat praktis dari penelitian ini. Dengan menggabungkan BERT ke dalam SIEM, risiko pencurian data pribadi, gangguan layanan, dan penyebaran *malware* dapat diminimalisir. Sebagai hasilnya, penerapan sistem ini diharapkan menurunkan tingkat insiden siber, meningkatkan kepercayaan pengguna terhadap layanan online, dan meningkatkan kesadaran proaktif masyarakat tentang keamanan informasi.

b) Manfaat bagi Peneliti

Salah satu manfaat bagi peneliti dari penelitian ini adalah meningkatkan kemampuan bidang informatika dalam bidang keamanan siber dengan menerapkan dan menerapkan metode *machine learning* untuk mendeteksi URL berbahaya yang berbahaya pada jaringan.

c) Manfaat bagi Ilmu Pengetahuan

Salah satu manfaat bagi ilmu pengetahuan dalam penelitian ini, yaitu melakukan implementasi *Security Information & Event Management*

*(*SIEM*)* untuk deteksi URL *berbahaya* pada koneksi jaringan yang berbahaya dan dapat mencegah adanya akses yang dapat membahayakan data pengguna pada jaringan. Peneliti juga berharap penelitian ini dapat menjadi referensi untuk penelitian berikutnya.

1.5 Kebaruan

Penelitian ini memberikan kebaruan berupa integrasi Large Language Model (LLM) berbasis BERT untuk meningkatkan akurasi pengolahan data dan melatih model dalam mengidentifikasi URL berbahaya, serta implementasi *Security Information & Event Management* (SIEM) yang memanfaatkan BERT dalam mendeteksi dan memblokir URL berbahaya secara otomatis pada jaringan lokal (LAN).

1.6 Kerangka Penulisan

Laporan ini disusun berdasarkan pedoman yang sudah ditetapkan oleh Lembaga Penjamin Mutu Universitas Pembangunan Jaya, dan sesuai dengan sistematika dalam Program Studi Informatika, yang terdiri dari 6 bab.;

BAB I PENDAHULUAN

Bab ini terdiri dari subab latar belakang dilakukannya penelitian, identifikasi masalah yang berupa rumusan masalah, tujuan penelitian, manfaat penelitian bagi masyarakat, peneliti, dan ilmu pengetahuan, kebaruan, dan kerangka penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini terdiri dari sub bab pencapain terdahulu dan tinjauan teoritis yang mendukung penelitian.

BAB III TAHAPAN PELAKSANAAN

Bab ini menjelaskan tahapan yang diperlukan untuk menjalankan penelitian dari awal hingga akhir, dan juga akan menjelaskan metode penelitian yang dipilih.

BAB IV PERANCANGAN

Bab ini menjelaskan tahapan yang dilakukan untuk melakukan pengembangan pada penelitian ini, berisi bagaimana sistem dan metode yang digunakan untuk mencapai hasil akhir.

BAB V HASIL DAN PEMBAHASAN

Bab ini akan membahas hasil dan temuan penelitian dan memberikan penjelasan tentang temuan dalan sistem yang dikembangkan.

BAB VI KESIMPULAN

Bab ini akan memuat hasil penelitian yang disusun secara sistematis tetapi juga memberikan rekomendasi untuk pengembangan selanjutnya.

.