BAB I

PENDAHULUAN

1.1. LATAR BELAKANG PEMIKIRAN MAGANG

Magang merupakan salah satu bentuk implementasi pembelajaran yang bertujuan untuk memberikan pengalaman kerja secara langsung kepada mahasiswa agar mampu mengaplikasikan ilmu yang telah diperoleh selama perkuliahan ke dalam dunia kerja. Melalui kegiatan magang, mahasiswa tidak hanya memperoleh pengalaman praktis, tetapi juga memahami proses kerja, budaya organisasi, serta tantangan yang dihadapi oleh suatu instansi dalam menjalankan tugas dan fungsinya. Kegiatan ini diharapkan dapat meningkatkan kompetensi, kemampuan analisis, serta keterampilan mahasiswa dalam menyelesaikan permasalahan yang terjadi di lingkungan kerja.

Penulis melaksanakan kegiatan magang di Dinas Komunikasi, Informatika, Statistik, dan Persandian (DISKOMINFOTIK) Kabupaten Kepulauan Meranti, tepatnya pada Bidang Aplikasi Informatika. Bidang ini memiliki peran penting dalam pengembangan, pengelolaan, serta pemeliharaan sistem informasi dan teknologi informasi yang digunakan oleh pemerintah daerah. Seiring dengan meningkatnya pemanfaatan teknologi informasi dalam pelayanan publik, aspek keamanan jaringan menjadi salah satu hal yang sangat penting untuk diperhatikan guna menjaga kerahasiaan, integritas, dan ketersediaan data.

Alasan penulis memilih DISKOMINFOTIK Kabupaten Kepulauan Meranti sebagai tempat pelaksanaan magang karena instansi ini merupakan pusat pengelolaan teknologi informasi dan komunikasi di lingkungan Pemerintah Kabupaten Kepulauan Meranti. Selain itu, bidang yang ditempati memiliki keterkaitan yang sangat erat dengan kompetensi yang dipelajari pada Program Studi Rekayasa Perangkat Lunak, khususnya dalam bidang pengembangan perangkat lunak, keamanan sistem informasi, analisis data, serta penerapan kecerdasan buatan (*Artificial Intelligence*) dalam penyelesaian permasalahan nyata. Melalui kegiatan

magang ini, penulis memiliki kesempatan untuk mengembangkan kemampuan teknis sekaligus memperoleh pengalaman bekerja pada lingkungan pemerintahan.

Selama pelaksanaan magang, penulis mengidentifikasi bahwa salah satu permasalahan yang dihadapi adalah belum optimalnya sistem keamanan jaringan. Monitoring aktivitas jaringan masih memerlukan pengawasan secara berkala sehingga berpotensi menyebabkan keterlambatan dalam mendeteksi aktivitas yang tidak normal atau indikasi serangan siber. Kondisi tersebut dapat meningkatkan risiko terhadap keamanan infrastruktur teknologi informasi, seperti akses tidak sah, penyalahgunaan layanan jaringan, maupun ancaman lainnya yang dapat mengganggu operasional sistem pemerintahan.

Apabila kondisi tersebut tidak ditangani dengan baik, berbagai kerugian dapat terjadi, antara lain terganggunya ketersediaan layanan publik berbasis digital, meningkatnya risiko kebocoran informasi penting, kerusakan data, hingga menurunnya kepercayaan masyarakat terhadap layanan teknologi informasi yang disediakan oleh pemerintah daerah. Selain itu, proses identifikasi insiden keamanan yang dilakukan secara manual memerlukan waktu yang lebih lama sehingga respons terhadap ancaman menjadi kurang efektif.

Berdasarkan permasalahan tersebut, penulis mengusulkan pembangunan Network Intrusion Detection System (NIDS) yang memanfaatkan algoritma XGBoost sebagai metode utama untuk melakukan klasifikasi aktivitas jaringan normal dan aktivitas yang terindikasi sebagai serangan. Untuk meningkatkan kemampuan sistem dalam mengenali pola-pola ancaman tertentu, metode tersebut dikombinasikan dengan deteksi berbasis logika heuristik sehingga sistem tidak hanya mengandalkan hasil prediksi model *machine learning*, tetapi juga menggunakan aturan-aturan tertentu dalam mengidentifikasi aktivitas yang mencurigakan. Pendekatan gabungan ini diharapkan mampu meningkatkan akurasi deteksi sekaligus mengurangi kemungkinan kesalahan klasifikasi.

Pendekatan penggabungan algoritma XGBoost dengan logika heuristik ini juga sejalan dengan sejumlah penelitian terdahulu. Kombinasi algoritma heuristik dengan XGBoost dinilai efektif dalam secara adaptif mencari struktur parameter yang optimal, sehingga mampu mengenali kategori serangan minoritas yang sering

kali lolos dari sistem deteksi konvensional [1]. Arsitektur deteksi intrusi berbasis algoritma boosting yang dikolaborasikan dengan aturan penyaringan awal (heuristic rule) juga terbukti mampu menjaga kestabilan jaringan dari berbagai variasi pola serangan baru [2]. Selain itu, pendekatan hibrida atau gabungan berbasis aturan (rule-based/heuristik) dinilai diperlukan untuk menangani pola lalu lintas jaringan lokal pada instansi pemerintah guna menurunkan tingkat kesalahan alarm (false alarm rate) [3], sebagaimana yang menjadi konteks penerapan sistem pada DISKOMINFOTIK Kabupaten Kepulauan Meranti.

Selain itu, sistem yang dikembangkan juga dilengkapi dengan dashboard monitoring yang memungkinkan administrator memantau kondisi jaringan secara lebih mudah melalui visualisasi data, informasi lalu lintas jaringan, status aktivitas, serta notifikasi terhadap indikasi serangan yang terdeteksi. Dashboard tersebut diharapkan dapat membantu proses pengambilan keputusan secara lebih cepat sehingga penanganan terhadap potensi ancaman keamanan jaringan dapat dilakukan secara lebih efektif.

Melalui pelaksanaan magang ini, penulis berharap dapat memberikan kontribusi berupa solusi yang mampu mendukung peningkatan keamanan jaringan di lingkungan DISKOMINFOTIK Kabupaten Kepulauan Meranti sekaligus menerapkan ilmu yang telah diperoleh selama perkuliahan ke dalam penyelesaian permasalahan nyata di dunia kerja. Pengalaman yang diperoleh selama kegiatan magang juga diharapkan dapat menjadi bekal dalam menghadapi tantangan di dunia profesional setelah menyelesaikan pendidikan.

1.2. TUJUAN DAN MANFAAT MAGANG

Pelaksanaan magang ini memiliki tujuan dan manfaat tertentu, baik bagi penulis secara pribadi maupun bagi pihak-pihak yang terlibat di dalamnya. Adapun tujuan dan manfaat dari kegiatan magang ini adalah sebagai berikut.

1.2.1. Tujuan Magang

Tujuan yang ingin dicapai penulis melalui pelaksanaan magang ini antara lain:

1. Menerapkan dan mengembangkan ilmu pengetahuan serta keterampilan yang telah diperoleh selama perkuliahan, khususnya di bidang keamanan jaringan dan penerapan kecerdasan buatan, ke dalam penyelesaian permasalahan nyata di dunia kerja.
2. Memperoleh pengalaman kerja secara langsung di lingkungan instansi pemerintahan, khususnya dalam pengelolaan teknologi informasi dan komunikasi di DISKOMINFOTIK Kabupaten Kepulauan Meranti.
3. Melatih kemampuan analisis, pemecahan masalah, serta pengambilan keputusan dalam menghadapi permasalahan teknis yang terjadi di lingkungan kerja.
4. Merancang dan membangun purwarupa Network Intrusion Detection System (NIDS) berbasis XGBoost dan logika heuristik sebagai bentuk kontribusi nyata bagi peningkatan keamanan jaringan di DISKOMINFOTIK Kabupaten Kepulauan Meranti.

1.2.2. Manfaat Magang

a. **Bagi Penulis** Menambah wawasan dan pengalaman kerja nyata di instansi pemerintahan, meningkatkan kemampuan teknis di bidang keamanan jaringan dan machine learning, serta melatih kemampuan komunikasi, kerja sama tim, dan kedisiplinan dalam lingkungan kerja profesional.

b. **Bagi Program Studi** Menjadi sarana evaluasi kesesuaian kurikulum dengan kebutuhan dunia kerja, serta mempererat kerja sama antara Program Studi Rekayasa Perangkat Lunak Politeknik Negeri Bengkalis dengan DISKOMINFOTIK Kabupaten Kepulauan Meranti.

c. **Bagi Instansi** Memperoleh masukan berupa purwarupa solusi keamanan jaringan yang dapat menjadi bahan pertimbangan bagi DISKOMINFOTIK Kabupaten Kepulauan Meranti dalam pengembangan sistem monitoring keamanan jaringan di masa mendatang.

1.3 LUARAN PROYEK MAGANG

Luaran yang dihasilkan dari pelaksanaan magang ini berupa purwarupa (prototype) Network Intrusion Detection System (NIDS) yang mengombinasikan algoritma XGBoost dengan logika heuristik untuk mendeteksi aktivitas jaringan yang mencurigakan. Secara rinci, luaran proyek magang yang akan diserahterimakan kepada DISKOMINFOTIK Kabupaten Kepulauan Meranti meliputi:

1. Aplikasi/dashboard NIDS dalam bentuk purwarupa yang menampilkan hasil klasifikasi aktivitas jaringan (normal/serangan) secara real-time, dilengkapi visualisasi lalu lintas jaringan dan notifikasi indikasi serangan.
2. Model klasifikasi berbasis algoritma XGBoost yang telah dilatih menggunakan data lalu lintas jaringan, serta modul deteksi berbasis logika heuristik untuk mengenali pola-pola serangan tertentu.
3. Dokumentasi teknis sistem, mencakup arsitektur sistem, alur kerja (workflow), serta panduan instalasi dan penggunaan.
4. Laporan hasil pengujian dan evaluasi kinerja sistem sebagai bahan pertimbangan untuk pengembangan lebih lanjut.

Pada saat laporan ini disusun, luaran tersebut masih berupa purwarupa yang belum diimplementasikan secara langsung pada jaringan produksi DISKOMINFOTIK Kabupaten Kepulauan Meranti, sehingga diharapkan dapat menjadi dasar pengembangan lebih lanjut apabila akan diterapkan secara operasional di kemudian hari.