BAB 1. PENDAHULUAN

1.1 Latar Belakang

Di era digital yang semakin maju, sistem informasi dan jaringan komputer telah menjadi fondasi utama dalam menjalankan aktivitas pemerintahan, bisnis, pendidikan, hingga kehidupan sosial masyarakat. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi digital, ancaman terhadap keamanan siber pun kian kompleks dan membahayakan. Keamanan siber tidak lagi hanya menjadi isu teknis, melainkan sudah masuk ke ranah strategis dan nasional. Di Indonesia, urgensi untuk memperkuat sistem keamanan siber menjadi semakin mendesak, seiring dengan meningkatnya volume serangan digital yang menyasar berbagai sektor, mulai dari pemerintahan, finansial, hingga institusi pendidikan.

Menurut laporan resmi dari Badan Siber dan Sandi Negara (BSSN), lebih dari 300 juta anomali trafik jaringan terdeteksi hanya dalam kurun waktu satu tahun. Ironisnya, sebagian besar dari anomali tersebut tidak dapat ditindaklanjuti secara cepat karena lemahnya sistem deteksi dini dan keterbatasan sumber daya teknis di banyak institusi. Di sektor pendidikan, situasinya tidak jauh berbeda. Banyak lembaga masih mengandalkan sistem keamanan dasar tanpa kemampuan untuk memantau trafik jaringan secara real-time atau mendeteksi pola serangan yang kompleks. Hal ini memperlihatkan pentingnya pengembangan sistem keamanan yang bersifat cerdas, adaptif, dan berbasis data secara komprehensif.

Salah satu solusi yang telah dikaji dan menunjukkan potensi besar dalam penguatan keamanan jaringan adalah penggunaan Elastic Stack sebagai alat monitoring trafik. Elastic Stack memungkinkan pengumpulan, pengolahan, dan visualisasi data jaringan secara real-time, sehingga membantu pengambil keputusan dalam mengidentifikasi dan merespons ancaman siber secara cepat. Penelitian oleh Admi & Maulana (2020) menunjukkan bahwa sistem berbasis Elastic Stack dapat memberikan peningkatan signifikan dalam hal transparansi dan visibilitas data trafik, serta mampu mendukung deteksi anomali secara efisien

dan ekonomis, terutama di lingkungan yang memiliki keterbatasan sumber daya seperti lembaga pendidikan.

Selain aspek teknologi, kesiapan institusi dalam menerapkan standar keamanan informasi juga menjadi faktor kunci. Penelitian oleh Jelita et al. (2024) yang menggunakan pendekatan ISO/IEC 27001 menemukan bahwa sebagian besar lembaga pendidikan di Indonesia masih berada pada tingkat kesiapan rendah dalam hal pengendalian akses, manajemen risiko digital, dan kesadaran pengguna terhadap ancaman siber. Ketiadaan kerangka kerja keamanan yang terstruktur menjadi penghambat utama dalam membangun sistem perlindungan informasi yang efektif. Oleh karena itu, dibutuhkan pendekatan sistemik yang mencakup kebijakan, edukasi, serta adopsi teknologi yang relevan untuk menciptakan lingkungan digital yang aman.

Lebih lanjut, studi oleh Purba & Mauluddin (2023) menunjukkan bahwa kebocoran data digital yang terjadi di Indonesia sebagian besar disebabkan oleh lemahnya sistem monitoring lalu lintas data serta kurangnya integrasi analisis berbasis data dalam pengambilan keputusan keamanan. Hal ini membuktikan bahwa pendekatan keamanan konvensional yang reaktif dan statis sudah tidak memadai untuk menghadapi dinamika ancaman siber modern. Dibutuhkan sistem keamanan siber yang bersifat prediktif dan berbasis analitik, di mana Big Data Analytics berperan sebagai mesin utama dalam pengolahan data besar secara real-time untuk mendeteksi potensi ancaman sebelum menjadi insiden yang merugikan.

Di sisi lain, pendekatan heuristik yang bersifat adaptif dan berbasis pengalaman juga menunjukkan potensi besar dalam memperkuat sistem keamanan informasi. Meskipun belum banyak digunakan secara eksplisit dalam konteks keamanan siber Indonesia, metode ini terbukti efektif dalam deteksi kelemahan sistem dan pengambilan keputusan berbasis pola perilaku. Penelitian Nahas & Hustinawati (2023) yang menerapkan evaluasi heuristik terhadap sistem informasi DPR RI, menunjukkan bahwa metode ini mampu mengidentifikasi kelemahan secara cepat dan efisien. Hal ini sangat relevan jika diimplementasikan dalam konteks deteksi anomali jaringan dan keamanan trafik, terutama dalam institusi

yang membutuhkan sistem cepat dan fleksibel tanpa ketergantungan penuh pada machine learning kompleks.

Sebagai institusi pendidikan berbasis digital, merupakan lingkungan yang sangat tepat untuk penerapan sistem keamanan siber cerdas berbasis Big Data dan heuristik. Dengan tingginya aktivitas pembelajaran berbasis daring, penggunaan perangkat digital yang masif, serta ketergantungan terhadap jaringan internet, institusi ini berisiko tinggi menjadi target serangan siber. Oleh karena itu, dibutuhkan solusi yang adaptif, ekonomis, dan dapat dikembangkan secara mandiri oleh tim internal, tanpa bergantung pada vendor komersial mahal.

Berdasarkan uraian di atas, penelitian mengenai penerapan Big Data Analytics yang dikombinasikan dengan pendekatan heuristik untuk sistem keamanan siber dalam konteks lembaga pendidikan menjadi sangat relevan dan strategis. Selain memberikan kontribusi teknis terhadap penguatan sistem keamanan, penelitian ini juga mendukung kebijakan nasional dalam mewujudkan kedaulatan digital dan ketahanan siber yang berkelanjutan. Dengan adanya sistem monitoring trafik yang adaptif, institusi pendidikan dapat meningkatkan respons terhadap ancaman, mengurangi risiko kebocoran data, dan membentuk budaya keamanan digital yang lebih kuat di masa depan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana pemanfaatan *Big Data Analytics* dapat membantu dalam pengelolaan dan pemantauan traffic jaringan sebagai bagian dari sistem keamanan siber di lingkungan lembaga pendidikan?
2. Bagaimana metode heuristik dapat diterapkan untuk mendeteksi ancaman siber secara lebih efisien dan adaptif dalam sistem jaringan?
3. Sejauh mana efektivitas integrasi *Big Data Analytics* dengan metode heuristik dalam memperkuat sistem keamanan siber ?

1.3 Tujuan Penelitian

Penelitian ini memiliki tujuan sebagai berikut:

1. Untuk menganalisis penerapan *Big Data Analytics* dalam sistem manajemen traffic jaringan yang berkaitan dengan keamanan siber.
2. Untuk mengkaji efektivitas metode heuristik dalam mendeteksi anomali dan potensi serangan siber dalam lingkungan jaringan pendidikan.
3. Untuk merancang dan mengevaluasi model integrasi *Big Data Analytics* dengan metode heuristik dalam sistem keamanan siber.

1.4 Manfaat Penelitian

1. **Manfaat Teoritis:**

   Penelitian ini diharapkan dapat memperkaya kajian ilmiah di bidang keamanan siber, khususnya dalam penggabungan pendekatan Big Data Analytics dan metode heuristik. Hasil penelitian ini juga diharapkan dapat menjadi referensi akademis bagi penelitian lanjutan di bidang yang sama.
2. **Manfaat Praktis:**

   Penelitian ini diharapkan dapat memberikan kontribusi nyata bagi pengembangan sistem keamanan jaringan di lingkungan pendidikan.