**BAB 1**

**PENDAHULUAN**

* 1. **Latar Belakang**

Seiring dengan perkembangan teknologi internet dan komputer saat ini hampir semua orang menggunakan teknologi komputer dan internet. Berkat kemajuan tersebut banyak kebutuhan serta pekerjaan dengan mudah dapat dikerjakan dan secara tidak langsung hal ini telah menjadi fondasi esensial yang sangat berpengaruh bagi kelangsungan berbagai sektor kehidupan manusia. Adapun aspek yang cenderung memiliki ketergantungan terhadap infrastruktur teknologi internet dan komputer adalah aspek bisnis, pendidikan dan komunikasi. Dalam dunia pendidikan sendiri Universitas Islam Darul Ulum (UNISDA), mengandalkan sistem informasi untuk mendukung proses administrasi, akademik, dan operasional. Sistem informasi ini mencakup pengelolaan data mahasiswa, staf, keuangan, dan berbagai layanan berbasis teknologi yang menjadi tulang punggung dalam meningkatkan efisiensi dan kualitas layanan pendidikan. Namun, dengan ketergantungan yang tinggi terhadap teknologi informasi, muncul pula risiko keamanan data, termasuk ancaman terhadap integritas, kerahasiaan, dan ketersediaan informasi. Hal ini mengakibatkan, keamanan siber dan perlindungan terhadap berbagai serangan telah menjadi pertanyaan yang mendesak pada saat ini. Alasan utama dibalik hal tersebut adalah pertumbuhan dan ketergantungan terhadap penggunaan internet dan jaringan komputer sehingga potensi kejahatan oleh orang yang tidak bertanggung jawab dapat memanfaatkan momentum ini untuk melakukan sebuah penyerangan sehingga dapat menjadi keuntungan bagi orang yang tidak bertanggung jawab tersebut. Serangan siber dapat menyebabkan kerusakan yang signifikan parah dan dapat menimbulkan kerugian finansial yang signifikan dalam jaringan skala besar (Prabuningrat et al., 2024)

Seperti yang diketahui, siber sekuriti adalah sebuah kumpulan teknologi, teknik, proses dan kebijakan yang bekerja bersama dan di desain untuk melindungi komputer, jaringan, software program dan data dari serangan dan akses, perubahan dan perusakan yang tidak sah. Oleh karena itu, mengingat hal ini menjadi sangat krusial maka diperlukan cara yang akan berperan penting dalam keamanan saat ini untuk mendeteksi berbagai serangan siber atau anomali dalam sebuah jaringan serta pengembangan sistem deteksi intrusi yang efektif dan efisien. Teknik-teknik kecerdasan buatan (AI), terutama dalam bentuk machine learning dapat dimanfaatkan untuk merancang sistem deteksi intrusi yang cerdas berbasis data. Pada awal penelitian tentang deteksi anomali banyak didasari dengan penggunaan metode *signature based*. Namun hal ini memiliki kendala yang patut diperhitungkan yaitu harus selalu dilakukan perbaharui terkini pada basis data jika signature baru muncul. Metode ini berhasil dalam mendeteksi serangan yang sudah teridentifikasi sebelumnya, namun tidak efektif dalam menghadapi serangan yang belum diketahui. Sementara itu, deteksi anomali mengandalkan mekanisme heuristic untuk mengenali aktivitas berbahaya yang belum teridentifikasi sebelumnya. Maka, diperlukan lebih banyak penelitian untuk mengembangkan teknik deteksi anomali lalu lintas jaringan yang menggunakan klasifikasi machine learning yang lebih mutakhir agar dapat menemukan jenis anomali yang baru.

Menurut (Wardhani, 2024) Salah satu pendekatan yang telah menjadi fokus penelitian dalam deteksi intrusi pada jaringan komputer adalah penggunaan teknik *machine learning* . *Machine learning* memungkinkan sistem untuk belajar dari data dan mengidentifikasi pola yang mencurigakan atau aneh dalam lalu lintas jaringan. Penggunaan teknik machine learning dalam deteksi intrusi dapat meningkatkan kemampuan sistem untuk mendeteksi serangan yang tidak diketahui atau yang tidak sesuai dengan pola serangan yang sudah dikenal, dalam konteks ini, penggunaan teknik klasifikasi merupakan salah satu pendekatan yang umum digunakan dalam deteksi intrusi. Teknik ini memungkinkan sistem untuk mengklasifikasikan aktivitas jaringan sebagai normal atau mencurigakan berdasarkan pola yang telah dipelajari dari data pelatihan. Teknik klasifikasi dalam deteksi intrusi telah berhasil dalam mengenali pola serangan dengan tingkat akurasi yang tinggi. Selain teknik klasifikasi, pendekatan berbasis anomaly detection juga sering digunakan dalam deteksi intrusi pada jaringan komputer Pendekatan ini bertujuan untuk mengidentifikasi perilaku yang tidak biasa atau anomali dalam lalu lintas jaringan yang mungkin merupakan tanda adanya serangan.

Deteksi anomali memeriksa titik data tertentu dan mendeteksi kejadian langka yang tampak mencurigakan karena berbeda dengan pola perilaku yang ada. Deteksi anomali bukanlah hal baru, tetapi seiring dengan bertambahnya data, pelacakan manual menjadi tidak praktis. Deteksi anomali sangat penting di industri, seperti keuangan, ritel, dan keamanan siber, tetapi setiap bisnis harus mempertimbangkan solusi deteksi anomali. Deteksi anomali menyediakan cara untuk secara otomatis mendeteksi outlier yang berbahaya dan melindungi data Anda. Misalnya, perbankan adalah industri yang mendapatkan manfaat dari deteksi anomali. Dengan menggunakan deteksi anomali, bank dapat mengidentifikasi aktivitas penipuan dan pola yang tidak konsisten serta melindungi data. Data adalah jalur kehidupan bisnis Anda, dan menyepelekan data ini dapat membahayakan operasi Anda. Tanpa deteksi anomali, Anda dapat kehilangan pendapatan dan ekuitas merek yang membutuhkan waktu bertahun-tahun untuk dikembangkan. Bisnis Anda mengalami pelanggaran keamanan dan kehilangan informasi sensitif pelanggan.  Jika hal ini terjadi, Anda akan kehilangan tingkat kepercayaan pelanggan yang mungkin tidak dapat dikembalikan (Bororing, 2024).

Penelitian yang pernah dilakukan oleh (Bororing, 2024) dengan judul penelitian “Pengembangan Algoritma Machine Learning Untuk Mendeteksi Anomali Dalam Jaringan Komputer” dalam rangka mengatasi ancaman serangan anomali dalam jaringan komputer, penelitian ini merinci kemajuan terkini dalam pengembangan algoritma machine learning. Analisis literatur mengungkapkan kompleksitas dan variasi metode deteksi, serta menyoroti tantangan dan peluang yang muncul. Kesimpulan menegaskan bahwa pemahaman lebih lanjut terhadap aspek teknis dan implementasi praktis algoritma machine learning dapat memperkuat pertahanan terhadap serangan anomali di lingkungan jaringan komputer.

Perkembangan teknologi menjadi semakin penting karena memberikan alat dan teknik yang lebih canggih dan efektif untuk menemukan tindakan yang mencurigakan. Transformasi digital akan meminimalkan kecurangan. *Machine learning,* menjadi metode yang inovatif untuk meningkatkan deteksi anomali dengan memanfaatkan kemampuan komputasi yang kuat untuk menganalisis data secara tepat dan akurat. Dengan demikian, penggunaan teknologi ini membuka peluang baru untuk meningkatkan efektivitas dalam mengidentifikasi dan mencegah kecurangan dalam audit sistem informasi.

Permasalahan diatas merupakan alasan penulis untuk melakukan penelitian dengan judul “Penerapan Algoritma Machine Learning untuk Deteksi Anomali Dalam Audit Sistem Informasi di Lingkungan Universitas Islam Darul Ulum.

**Formulasi Permasalahan Penelitian**

* **Permasalahan Utama:**

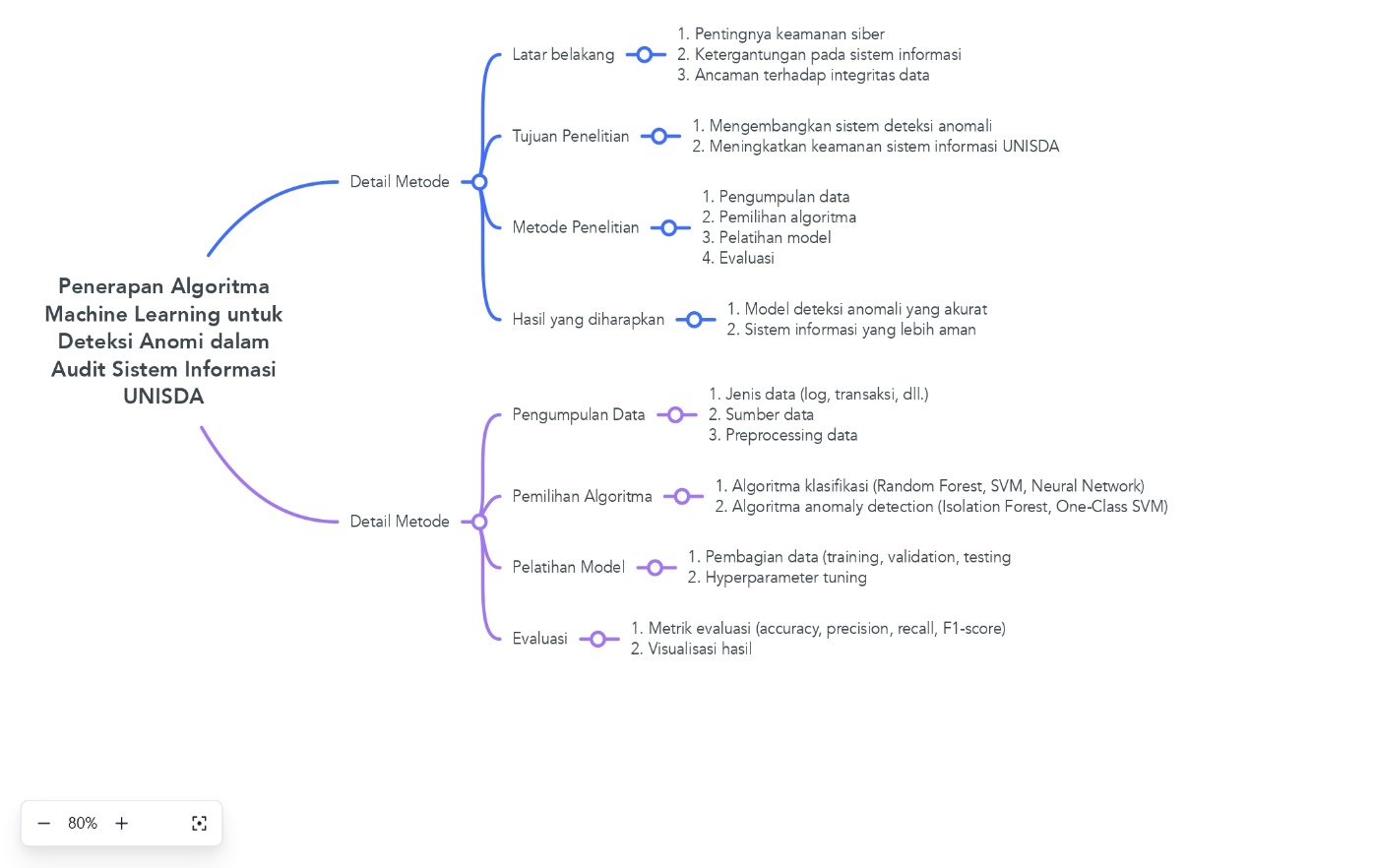
Bagaimana algoritma machine learning dapat diterapkan secara efektif untuk mendeteksi anomali dalam audit sistem informasi di lingkungan Universitas Islam Darul Ulum sehingga dapat meningkatkan keamanan dan integritas data?

* **Permasalahan Khusus:**

1. Algoritma machine learning mana yang paling tepat untuk diterapkan dalam konteks deteksi anomali pada sistem informasi UNISDA, dengan mempertimbangkan jenis data dan karakteristik serangan yang mungkin terjadi?
2. Bagaimana cara mengevaluasi kinerja model machine learning yang telah dikembangkan dalam mendeteksi berbagai jenis anomali, seperti serangan intrusi, akses tidak sah, dan perubahan data yang tidak wajar?
3. Faktor-faktor apa saja yang mempengaruhi akurasi dan efisiensi model machine learning dalam mendeteksi anomali pada sistem informasi UNISDA?

**Research Gap:**

1. **Penelitian Terdahulu:** Mayoritas penelitian terdahulu fokus pada deteksi anomali dalam jaringan komputer secara umum, belum spesifik pada audit sistem informasi di lingkungan pendidikan seperti UNISDA.
2. **Jenis Data**: Penelitian ini perlu mempertimbangkan jenis data yang spesifik pada sistem informasi UNISDA, seperti data akademik, keuangan, dan administrasi.
3. **Algoritma:** Perlu dilakukan perbandingan kinerja berbagai algoritma machine learning untuk menemukan algoritma yang paling cocok dengan karakteristik data UNISDA.
4. **Evaluasi**: Perlu dikembangkan metrik evaluasi yang komprehensif untuk mengukur kinerja model machine learning dalam mendeteksi berbagai jenis anomali.

Mind Mapping dari referensi yg digunakan.

**Metode yg diusulkan dan Rencana Metrik Pengujian yg digunakan**

1. **Systematic Literature Review (SLR):**

* Menyusun data dari jurnal nasional dan internasional yang relevan.
* Fokus pada metode machine learning dalam deteksi anomali dan tata kelola berbasis COBIT 5.
* Tahapan SLR: pencarian jurnal, evaluasi kualitas, ekstraksi data, dan analisis sintesis.

1. **Eksperimen Algoritma Machine Learning:**

* Dataset: Data riwayat dari sistem audit Universitas (jika tersedia) atau dataset open-source untuk deteksi anomali.
* Algoritma:
  + Supervised Learning: Random Forest, SVM
  + Unsupervised Learning: DBSCAN, K-Means
  + Ensemble Models: Bagging, Boosting

**Rencana Metrik Pengujian:**

1. **Akurasi (Accuracy):** Seberapa baik model mendeteksi anomali vs. non-anomali.
2. **Precision:** Kemampuan model menghindari false positive.
3. **Recall:** Kemampuan mendeteksi semua kasus anomali yang benar.
4. **F1-Score:** Kombinasi dari precision dan recall.
5. **ROC-AUC Curve:** Evaluasi performa model secara keseluruhan.

**Daftar Pustaka**

Bororing, G. M. G. (2024). Pengembangan Algoritma Machine Learning Untuk Mendeteksi Anomali Dalam Jaringan Komputer. *Jurnal Review Pendidikan Dan …*, *7*, 1361–1368.

Prabuningrat, G. S. W., Hostiadi, D. P., & Srinadi, N. L. P. (2024). Klasifikasi Deteksi Anomali Menggunakan Metode Machine Learning. *Prosiding Seminar Hasil Penelitian Informatika Dan Komputer*, *1*(2), 845–850.

Wardhani, N. F. (2024). Penggunaan Machine Learning Dalam Deteksi Intrusi Pada Jaringan Komputer. *Duniadata.Org*, *1*(4), 1–16.