BAB I

PENDAHULUAN

1.1 Latar Belakang

Menurut laporan *IBM X-Force Threat Intelligence Index* 2025, serangan dengan kategori *Exploit Public-Facing Applications* menyumbang sekitar 30% dari total serangan siber yang terjadi sepanjang tahun 2023 dan 2024 (IBM, 2025). Meskipun laporan tersebut tidak merinci jenis serangannya, dalam *framework MITRE ATT&CK*, serangan terhadap aplikasi yang dapat diakses publik (*Public-Facing Applications*) umumnya menggunakan teknik seperti *SQL Injection (SQLIi, Command Injection,* dan *Path Traversal.* Diantara teknik-teknik tersebut, *SQL Injection* (T1190) merupakan salah satu yang paling umum digunakan (*MITRE ATT&CK*, 2024).

SQL Injection telah lama dikenal sebagai metode eksploitasi yang sangat efektif, terutama karena kemampuannya dalam memperoleh akses awal (*initial access*) ke sistem target tanpa otorisasi. Bahkan, kelompok ancaman nyata seperti *Agrius* dilaporkan menggunakan teknik ini dalam fase awal serangan mereka (*MITRE ATT&CK Group: Agrius, 2024*).

Meskipun upaya untuk mendeteksi serangan *SQL Injection* telah dilakukan melalui metode seperti *signature-based detection* atau analisis perilaku, pendekatan-pendekatan tersebut masih menghadapi keterbatasan signifikan, terutama dalam mengenali varian serangan yang kompleks atau telah disamarkan. Salah satu tantangan terbesar dalam mengembangkan sistem deteksi yang efektif adalah keterbatasan

dataset serangan yang representatif dan realistis. Kebutuhan akan data yang kaya dan bervariasi menjadi sangat penting untuk melatih model deteksi modern seperti *machine learning* atau *deep learning* agar mampu mengenali pola serangan yang belum pernah terlihat sebelumnya (Dasari et al., 2025).

Pembuatan dataset sintetis menjadi krusial dalam penelitian keamanan siber karena dataset publik yang tersedia saat ini, seperti NSL-KDD atau ISCX, sudah tidak relevan (*outdated*) terhadap variasi serangan modern dan sering kali mengalami masalah ketidakseimbangan data (data *imbalance*). Keterbatasan data asli yang bersifat sensitif dan privat juga menjadi hambatan dalam pengembangan sistem deteksi. Data sintetis berbasis *Generative Adversarial Networks* (GAN) diperlukan untuk menyediakan volume data yang besar dengan variasi serangan yang lebih luas, termasuk teknik penyamaran (*obfuscation*) baru yang mungkin belum terekam dalam dataset publik (Anande et al., 2023) (Dasari et al., 2025).

Hal ini didukung oleh penelitian Zeng, yang menyatakan bahwa ketergantungan pada dataset statis membatasi kemampuan adaptasi sistem keamanan terhadap teknik obfuscation baru pada SQL Injection. Oleh karena itu, diperlukan sebuah metode pengembangan dataset sintetis menggunakan *Generative Adversarial Networks* (GAN) yang mampu mereplikasi distribusi data asli namun tetap memberikan variabilitas fitur yang diperlukan untuk melatih model deteksi yang lebih adaptif (Arjovsky et al., 2017).

Terdapat penelitian sebelumnya yang dilakukan oleh Dasari dengan judul "*Enhancing SQL Injection Detection and Prevention Using Generative Models"* ,penelitian ini membuat pendekatan inovatif yang memanfaatkan model generatif

untuk meningkatkan mekanisme deteksi dan pencegahan *SQLi.* Dengan menggabungkan *Variational Autoencoders (VAE), Conditional Wasserstein GAN* dengan *Gradient Penalty (CWGAN-GP)*, dan *U-Net, query SQL* sintetis dihasilkan untuk memperbesar *dataset training* bagi model *Machine Learning*. Metode yang diusulkan berhasil meningkatkan akurasi deteksi SQLi dengan mengurangi *false positive dan false negative*. Pengujian menunjukkan sistem mampu beradaptasi dengan pola serangan yang berkembang, sehingga meningkatkan presisi dan ketahanan deteksi. Meskipun berhasil meningkatkan deteksi *SQL Injection* dengan berbagai model generatif, namun lebih menekankan pada sistem deteksi dan pencegahan, bukan pengembangan dataset lengkap (Dasari et al., 2025).

Penelitian terdahulu lainnya diteliti oleh Ammara dengan judul "*Synthetic Data Generation in Cybersecurity: A Comparative Analysis"*, Penelitian ini melakukan analisis komparatif teknik non-AI, AI konvensional, dan GAN untuk menghasilkan data tabular sintetis menggunakan *dataset* NSL-KDD dan CICIDS-2017. Hasil menunjukkan bahwa metode GAN, khususnya CTGAN dan CopulaGAN, lebih unggul dalam *fidelity* dan utilitas dibandingkan metode lain. Selain itu, penggunaan mutual information untuk seleksi fitur terbukti meningkatkan kualitas data sintetis. Temuan ini memberikan panduan penting bagi pemilihan metode generasi data sintetis dalam keamanan siber. Tetapi penelitian ini berfokus pada pembuatan fitur trafik jaringan yang realistis tanpa membangun dataset serangan tertentu (Ammara et al., 2024).

CTGAN dan *CWGAN-GP* dipilih berdasarkan penelitian *Modeling Tabular Data using Conditional GAN* oleh Lei Xu dan *Enhancing SQL Injection Detection and Prevention Using Generative Models* oleh *Dasari* (Xu et al., 2019) (Dasari et al., 2025).

Penelitian ini bertujuan untuk mengembangkan *dataset* serangan *SQL Injection* sintetis berbasis *GAN*. Penggunaan dataset statis seperti NSL-KDD dianggap tidak lagi representatif terhadap serangan modern. Oleh karena itu, diperlukan dataset sintetis sebagai landasan pelatihan model deteksi yang adaptif. *Dataset* yang akan dibangun adalah dataset yang merepresentasikan paket jaringan serangan *SQL Injection*. Data yang diolah terdiri dari dua bagian utama, yaitu *header paket* dan *payload query SQL Injection*. *Header* paket berisi informasi terstruktur seperti protokol *TCP/IP*, alamat *IP, port*, dan *flag*, yang bersifat tabular dengan fitur numerik dan kategorikal. Sedangkan *payload* adalah *query SQL* yang bersifat sekuensial dan berbasis teks dengan pola sintaks yang kompleks dan bervariasi (Anande et al., 2023).

Karena perbedaan karakteristik tersebut, penggunaan satu model *GAN* tunggal tidak cukup optimal untuk menghasilkan kedua jenis data ini secara bersamaan. Oleh karena itu, dalam penelitian ini akan digunakan dua model *GAN* yang berbeda sesuai dengan tipe data masing-masing. *CTGAN* untuk menghasilkan *dataset header* paket jaringan yang tabular dan kategorikal. *Conditional Wasserstein GAN with Gradient Penalty* (*CWGAN-GP*) untuk menghasilkan *dataset payload query SQL Injection*. *CWGAN-GP* dipilih karena kemampuan stabilitas *training* yang lebih baik dibanding *GAN* konvensional, serta efektivitasnya dalam menghasilkan data sekuensial dan teks yang realistis dan bervariasi (Arjovsky dkk., 2017).

Evaluasi dataset sintetis juga digunakan untuk mengevaluasi hasil generasi dataset sintetis menyerupai dataset asli dan juga stabil untuk digunakan, dengan uji *kolmogorov-smirnov* (KS test) digunakan untuk mengevaluasi fitur numerik kontinu dan *jensen-shannon divergence* (JSD) memberikan ukuran jarak distribusi probabilitas yang lebih simetris untuk fitur kategorikal (Nielsen, 2019).

Dengan pendekatan ini, diharapkan dapat mengatasi keterbatasan *dataset* asli dan memberikan kontribusi signifikan dalam pengembangan sistem deteksi serangan siber yang lebih adaptif dan akurat.

1.2 Rumusan Masalah

1. Bagaimana *CTGAN* dapat digunakan untuk menghasilkan data sintetis header paket jaringan yang bersifat tabular dan kategorikal, serta bagaimana *CWGAN-GP* dapat menghasilkan *query SQL* Injection sintetis yang valid pada bagian payload ?.
2. Bagaimana cara menggabungkan dataset *header* dan *payload* sintetis sehingga membentuk dataset paket jaringan lengkap yang realistis dan konsisten ?.

1.3 Tujuan Penelitian

1. Mengimplementasikan model *CTGAN* untuk menghasilkan data sintetis *header* paket jaringan yang merepresentasikan data tabular dan kategorikal, serta menerapkan *CWGAN-GP* untuk menghasilkan *payload* berupa *query SQL Injection* sintetis yang memiliki struktur syntax valid.

2. Membangun mekanisme integrasi antara dataset header dan payload sintetis menggunakan pustaka Scapy guna membentuk dataset paket jaringan utuh dalam format PCAP yang memenuhi kriteria realistis secara statistik dan konsisten secara protokol jaringan.

1.4 Manfaat Penelitian

1. Menyediakan *dataset* sintetis *SQL Injection* yang realistis dan beragam untuk melatih sistem deteksi serangan modern.
2. Meningkatkan ketahanan sistem deteksi terhadap varian serangan baru yang belum pernah terlihat sebelumnya.
3. Memberikan referensi implementasi *CTGAN* dan *CWGAN-GP* dalam konteks augmentasi data tabular dan sekuensial.
4. *Dataset* sintetis yang dihasilkan dapat diakses secara terbuka (*open-source*) untuk mendukung penelitian lanjutan.

1.5 Batasan Masalah

1. Hanya fokus pada serangan *SQL Injection* dan tidak mencakup jenis serangan aplikasi web lainnya.
2. Data *header* paket jaringan dibatasi pada protokol *TCP/IP* dengan fitur umum seperti alamat *IP*, *port*, dan *flag*.
3. Hanya menggunakan dua jenis model *GAN: CTGAN* untuk data tabular (header) dan CWGAN-GP untuk data sekuensial (payload).