Madani: **Jurnal Ilmiah Multidisipline**
Volume 3, Nomor 5, June 2025, P. 535-541
E-ISSN: 2986-6340
Licenced by CC BY-SA 4.0
DOI: https://doi.org/10.5281/zenodo.15707795

Optimalisasi Intelijen Ancaman Siber di Security Operation Centers dengan Pemanfaatan Large Language Models (LLM) dan SIEM

Rizki Ramadhani, Angella Christie, Alma Amira Dewani, Marselinus Krisnawan R., Rafif Dhimaz Ardhana
Fakultas Teknologi Elektro dan Informatika Cerdas, Institut Teknologi Sepuluh Nopember, Surabaya, 60111, email: 5027221013@mhs.its.ac.id, 5027221047@mhs.its.ac.id, 5027221054@mhs.its.ac.id, 5027221056@mhs.its.ac.id, 5027221066@mhs.its.ac.id

Abstract
In the era of increasing digital transformation, cyber threats have become a major concern for higher education institutions such as Institut Teknologi Sepuluh Nopember (ITS). Security Operations Center (SOC) plays a crucial role in detecting and responding to security incidents, often supported by Security Information and Event Management (SIEM) systems like Wazuh. However, traditional SIEM systems generate high volumes of alerts, many of which are false positives, causing alert fatigue and slowing incident response. This study explores the integration of Large Language Models (LLM), such as GPT-4 and LLaMA 3, to enhance SOC performance through intelligent triage automation. Using a qualitative descriptive approach based on literature review, this research proposes a conceptual system framework that combines SIEM with LLM as an analytical agent. The designed system features components for alert processing, natural language explanation, automated reporting, and a feedback loop for continuous improvement. The proposed framework is expected to reduce the workload of SOC analysts, improve alert classification accuracy, and accelerate threat response in academic environments.
Keywords: Security Operations Center (SOC), Large Language Model (LLM), SIEM, GPT-4, Wazuh

Article Info
Received date: 29 May 2025 Revised date: 05 June 2025 Accepted date: 18 June 2025

PENDAHULUAN

Dalam era transformasi digital yang semakin pesat, keamanan siber telah menjadi salah satu prioritas utama bagi berbagai institusi, termasuk perguruan tinggi seperti Institut Teknologi Sepuluh Nopember (ITS). Layanan akademik, data riset, serta informasi pribadi sivitas akademika menjadi sasaran empuk bagi berbagai bentuk ancaman siber, mulai dari serangan phishing hingga serangan yang disponsori oleh negara. Menurut laporan IBM Security (2023), sektor pendidikan menempati salah satu posisi teratas dalam daftar sektor dengan serangan siber terbanyak setiap tahunnya [1].

Sebagai garda depan pertahanan siber, Security Operations Center (SOC) bertanggung jawab dalam memantau, mendeteksi, dan merespons insiden keamanan secara real-time. Salah satu komponen utama SOC adalah sistem Security Information and Event Management (SIEM) seperti Wazuh, yang mampu mengumpulkan dan mengkorelasikan log keamanan dari berbagai sumber dalam jaringan. Namun, tantangan utama dari penggunaan SIEM konvensional adalah banyaknya alert yang bersifat false positive, serta tingginya kebutuhan analisis manual yang membebani analis SOC, khususnya di tingkat pertama (Tier 1) [2][3]. Hal ini menyebabkan alert fatigue, keterlambatan dalam deteksi ancaman aktual, serta risiko terlewatnya insiden berbahaya yang dapat mengganggu keberlangsungan layanan kampus.

Dalam kondisi ini, dibutuhkan pendekatan baru yang lebih adaptif dan cerdas dalam

mendukung kinerja SOC. Large Language Models (LLM) seperti GPT-4, LLaMA 3, dan OpenHermes telah menunjukkan kemampuan dalam memahami dan memproses informasi tidak terstruktur, termasuk log keamanan, serta memberikan klasifikasi, rekomendasi, dan penjelasan dalam bahasa alami [4][5]. Studi oleh Singh et al. (2024) menunjukkan bahwa integrasi LLM dengan SIEM dapat mempercepat proses triase alert hingga 40% dan menurunkan beban kerja analis sebesar 60%, dengan GPT-4 mencatat precision 94% dan F1-score 93% dalam klasifikasi alert [6].

Selain karena efisiensi teknis, pentingnya penelitian ini juga didorong oleh kesenjangan antara jumlah insiden keamanan dan ketersediaan analis SOC yang terlatih. Ketersediaan tenaga ahli keamanan siber di Indonesia masih sangat terbatas dibandingkan dengan volume ancaman yang terus meningkat. Menurut laporan dari BSSN (2023), terdapat lebih dari 403 juta anomali trafik yang terdeteksi dalam sistem pemerintahan dan pendidikan tinggi selama satu tahun, namun kapasitas sumber daya manusia masih belum mencukupi [7]. Dengan kondisi tersebut, integrasi teknologi berbasis kecerdasan buatan seperti LLM menjadi opsi strategis untuk membantu otomatisasi proses, mendukung pengambilan keputusan, dan meningkatkan respons terhadap insiden di institusi pendidikan seperti ITS.

Berdasarkan kondisi tersebut, penelitian ini bertujuan menyusun kerangka kerja konseptual integrasi LLM dan SIEM yang berpotensi diterapkan di SOC ITS. Pendekatan ini tidak hanya mengacu pada hasil studi terdahulu, tetapi juga menawarkan desain sistem yang adaptif dan dapat disesuaikan dengan kebutuhan operasional institusi pendidikan tinggi.

Penelitian oleh Y. Singh, N. Patel, dan S. K. Shandilya (2024) mengusulkan integrasi beberapa Large Language Models (LLM) seperti GPT-4, LLaMA 3, dan Mixtral ke dalam sistem SIEM (Wazuh) untuk meningkatkan efisiensi Security Operations Center (SOC). Framework yang dikembangkan mampu mengklasifikasikan alert sebagai actionable atau non-actionable, menyajikan penjelasan dalam bahasa alami, serta mengotomatiskan pelaporan insiden. Hasil uji coba menunjukkan bahwa penggunaan GPT-4 dapat meningkatkan akurasi klasifikasi hingga 94% precision dan mempercepat proses triase hingga 40%, sehingga mengurangi beban kerja analis keamanan secara signifikan [6].

TINJAUAN PUSTAKA

Security Operation Center (SOC)

Security Operations Center (SOC) adalah pusat kendali keamanan yang bertugas untuk memantau, mendeteksi, menganalisis, dan merespons ancaman keamanan siber dalam suatu organisasi. SOC berperan penting dalam menjaga keamanan sistem informasi dengan melakukan pengelolaan insiden keamanan serta analisis forensik jika terjadi pelanggaran keamanan [8].

Menurut Parker (2021), SOC biasanya terdiri dari berbagai komponen seperti pemantauan log, korelasi kejadian, serta respons terhadap insiden keamanan [9]. Dalam konteks perguruan tinggi seperti ITS, keberadaan SOC menjadi krusial untuk menjaga keamanan data akademik, sistem informasi mahasiswa, serta infrastruktur penelitian yang sensitif [3].

Security Information and Event Management (SIEM)

SIEM adalah bidang dalam keamanan komputer yang menggabungkan dua komponen utama, yaitu Security Information Management (SIM) dan Security Event Management (SEM). Integrasi ini memungkinkan analisis keamanan secara real-time terhadap alert yang dihasilkan oleh aplikasi, sistem operasi, dan perangkat jaringan [10][11]. SIEM menjadi komponen sentral dalam infrastruktur Security Operations Center (SOC) karena berperan dalam mendeteksi, menyelidiki, dan merespons insiden keamanan siber secara sistematis [12].

Teknologi SIEM mengumpulkan dan mengagregasikan data dari berbagai sistem dan sumber log untuk memungkinkan organisasi mendeteksi ancaman siber, sekaligus memenuhi kebutuhan kepatuhan terhadap regulasi keamanan. Menurut definisi dari National Institute of Standards and Technology (NIST), SIEM adalah aplikasi yang menyediakan kemampuan untuk mengumpulkan data keamanan dari berbagai komponen sistem informasi dan menyajikannya dalam bentuk informasi yang

dapat ditindaklanjuti melalui satu antarmuka terpusat [13].

Contoh implementasi SIEM adalah Wazuh, platform open-source yang menyediakan fitur monitoring log, analisis ancaman, pemantauan integritas file, dan compliance checking terhadap standar seperti PCI DSS, ISO 27001, atau GDPR. SIEM seperti Wazuh memungkinkan korelasi antar data dari berbagai sumber dan penggunaan aturan deteksi berbasis ancaman yang adaptif [14].

Large Language Models (LLM)

Large Language Models (LLM) adalah model kecerdasan buatan berbasis deep learning yang dilatih menggunakan corpus teks dalam skala besar dan dirancang untuk memahami, memproses, serta menghasilkan teks dalam bahasa alami. Hampir semua LLM modern (seperti seri GPT, Gemini, Llama, dll.) merupakan pengembangan dari arsitektur transformer, yang diperkenalkan oleh Vaswani et al. (2017) dalam paper berjudul Attention is All You Need, yang secara signifikan meningkatkan kemampuan model dalam memahami konteks bahasa melalui mekanisme self-attention [15].

Dalam konteks keamanan siber, LLM dapat digunakan untuk mendukung SOC dan SIEM dalam berbagai aspek, seperti: Analisis log keamanan: Memproses data log dalam jumlah besar untuk mendeteksi pola anomali [16] Deteksi ancaman berbasis NLP: Memahami deskripsi serangan dan membantu dalam otomatisasi klasifikasi insiden [17]. Otomatisasi laporan keamanan: Menghasilkan ringkasan insiden keamanan secara otomatis berdasarkan data yang dikumpulkan [18].

METODE

Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam mengenai tantangan operasional yang dihadapi Security Operations Center (SOC), khususnya dalam proses triase alert, serta untuk mengkaji potensi penerapan Large Language Models (LLM) dalam sistem keamanan informasi. Penelitian ini tidak melakukan pengujian langsung di sistem produksi, melainkan merancang sebuah kerangka sistem konseptual yang dapat diterapkan pada SOC di lingkungan Institut Teknologi Sepuluh Nopember (ITS).

Pengumpulan Data

Data yang digunakan dalam penelitian ini bersumber dari: Jurnal ilmiah dan publikasi peer-reviewed terkait SIEM, LLM, dan keamanan siber. Dokumentasi resmi dari lembaga seperti NIST, IBM Security, Ponemon Institute, dan BSSN, Laporan teknis dan whitepapers dari pengembang sistem SIEM dan model LLM, Studi kasus dan framework yang telah dikembangkan oleh peneliti sebelumnya, seperti Singh et al. (2024). Seluruh sumber dikumpulkan dan dipilih berdasarkan relevansi, kebaruan, serta validitasnya dalam mendukung tujuan penelitian.

Teknik Analisis Data

Data yang telah dikumpulkan dianalisis dengan metode analisis isi (content analysis), yaitu dengan menelaah struktur sistem SIEM dan LLM, mengidentifikasi kelebihan dan kekurangannya, serta mensintesis pendekatan-pendekatan yang sudah ada menjadi kerangka sistem baru yang sesuai dengan kebutuhan SOC ITS. Proses analisis juga mencakup studi perbandingan antar model LLM serta karakteristik integrasinya dengan sistem SIEM berbasis open-source seperti Wazuh.

Perancangan Sistem Konseptual

Perancangan sistem dalam penelitian ini bertujuan untuk mengusulkan sebuah kerangka kerja konseptual yang mengintegrasikan Large Language Models (LLM) ke dalam sistem Security Information and Event Management (SIEM) untuk mendukung efisiensi operasional Security Operations Center (SOC), khususnya dalam proses triase alert. Rancangan ini disusun berdasarkan studi literatur dan hasil sintesis dari penelitian sebelumnya, terutama oleh Singh et al. (2024), serta disesuaikan dengan kebutuhan institusi pendidikan tinggi seperti ITS.

Kerangka sistem yang diusulkan mengandalkan SIEM sebagai pusat pengumpulan dan korelasi

data log keamanan, sementara LLM berperan sebagai agen analitik cerdas yang mengklasifikasikan dan menjelaskan alert menggunakan pemrosesan bahasa alami. Perancangan ini dibagi menjadi lima komponen utama sebagai berikut:

SIEM (Wazuh): Mengumpulkan log dari berbagai sumber seperti endpoint, jaringan, cloud, dan sistem identitas, lalu melakukan korelasi antar data.

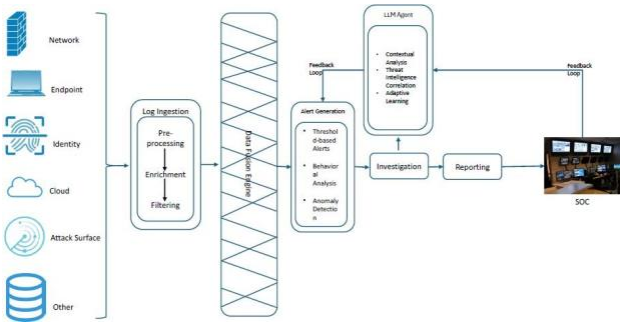
Alert Processing Engine: Menyaring dan mengelompokkan alert berdasarkan tingkat keparahan, jenis serangan, dan anomali perilaku.

LLM Agent: Menganalisis isi alert menggunakan teknik NLP dan NER, mengklasifikasikan alert menjadi actionable auto non-actionable, serta memberikan penjelasan berbasis konteks.

Reporting Module: Menyusun laporan insiden dalam bahasa alami yang mudah dipahami analis dan mendukung pelaporan terstandar.

Feedback Loop: Umpan balik dari analis SOC digunakan untuk melatih ulang atau menyesuaikan model secara adaptif, meningkatkan akurasi klasifikasi pada iterasi berikutnya.

Rancangan sistem divisualisasikan dalam Gambar 1, yang menunjukkan alur proses integrasi antara SIEM dan LLM dalam konteks operasional SOC.



Gambar 1. Integrasi multi-LLM ke dalam lingkungan SIEM untuk meningkatkan proses triase dalam Security Operations Centers (SOC

Pada gambar tersebut, data log berasal dari berbagai sumber keamanan seperti jaringan (network), endpoint, sistem identitas, cloud, dan permukaan serangan (attack surface) lainnya. Data log ini kemudian melalui tahap log ingestion yang mencakup pre-processing, enrichment, dan filtering sebelum diproses oleh modul korelasi dalam sistem SIEM.

SIEM menghasilkan alert berdasarkan tiga pendekatan utama, yaitu threshold-based alerts, behavioral analysis, dan anomaly detection. Alert yang dihasilkan dikirim ke LLM Agent, yang bertugas melakukan contextual analysis dan korelasi dengan threat intelligence, sekaligus menghasilkan penjelasan yang dapat ditindaklanjuti dalam bentuk laporan. Proses ini mendukung kegiatan investigasi insiden dan pelaporan dalam SOC.

Selanjutnya, SOC menerima laporan tersebut dan memberikan feedback terhadap hasil klasifikasi dan rekomendasi sistem. Feedback ini digunakan kembali oleh LLM untuk proses active learning, sehingga sistem mampu terus belajar dan beradaptasi terhadap pola ancaman baru di masa mendatang.

HASIL DAN PEMBAHASAN

Tantangan Utama yang Dihadapi SOC di Lingkungan Pendidikan Tinggi

Security Operations Center (SOC) pada institusi pendidikan tinggi seperti Institut Teknologi sepuluh Nopember (ITS) menghadapi berbagai tantangan dalam mendeteksi dan menangani insiden keamanan siber. Salah satu tantangan utama adalah volume alert yang sangat besar yang dihasilkan oleh sistem SIEM, dengan sebagian besar bersifat false positives. Hal ini menyebabkan alert fatigue,

yang dapat menurunkan responsivitas analis terhadap ancaman yang nyata.

Selain itu, keterbatasan jumlah tenaga analis dan kurangnya sistem pendukung otomatisasi memperburuk beban kerja, terutama pada Tier 1 SOC. Infrastruktur pendidikan juga seringkali memiliki kompleksitas sistem dan keberagaman perangkat yang tinggi, sehingga log yang dihasilkan sangat bervariasi dan tidak mudah dikorelasikan secara manual.

Studi oleh Ponemon Institute (2022) menunjukkan bahwa lebih dari 50% alert SIEM tidak ditindaklanjuti karena keterbatasan sumber daya manusia dan overload informasi, suatu kondisi yang relevan pula di lingkungan ITS.

Potensi Pemanfaatan LLM untuk Meningkatkan Efisiensi dan Akurasi

Large Language Models (LLM) seperti GPT-4, LLaMA 3, dan OpenHermes menawarkan pendekatan baru dalam mengelola dan menganalisis alert keamanan siber. Dengan kemampuan memahami konteks melalui pemrosesan bahasa alami (Natural Language Processing), LLM dapat digunakan untuk mengklasifikasikan alert ke dalam kategori yang relevan dan tidak relevan (actionable / non-actionable), serta menyusun penjelasan berbasis konteks yang membantu analisis lanjutan.

Penelitian oleh Singh et al. (2024) menunjukkan bahwa integrasi GPT-4 ke dalam SIEM mampu meningkatkan precision hingga 94% dan mengurangi waktu triase alert sebesar 40%. Dalam konteks ITS, pemanfaatan LLM dapat mengotomatisasi tugas berulang, mempercepat respons terhadap ancaman, dan mengurangi ketergantungan terhadap intervensi manual, sehingga meningkatkan efisiensi SOC secara keseluruhan.

Rancangan Sistem Konseptual Integrasi LLM dan SIEM

Berdasarkan hasil kajian literatur dan adaptasi terhadap kondisi SOC ITS, penelitian ini merancang kerangka sistem konseptual yang mengintegrasikan SIEM (seperti Wazuh) dengan LLM sebagai agen analitik cerdas. Sistem ini terdiri dari lima komponen utama:

1. SIEM untuk pengumpulan dan korelasi log,
2. Alert Processing Engine untuk menyaring alert berdasarkan prioritas,
3. LLM Agent untuk klasifikasi dan analisis berbasis konteks,
4. Reporting Module untuk penyusunan laporan insiden, dan
5. Feedback Loop untuk perbaikan model secara berkelanjutan.

Diagram sistem ini telah divisualisasikan pada Gambar 1. Desain ini memungkinkan otomatisasi triase alert sambil tetap mempertahankan supervisi manusia, sehingga cocok diterapkan pada institusi pendidikan yang memiliki keterbatasan sumber daya analis.

Rekomendasi Strategis untuk Penerapan SOC Berbasis AI

Agar integrasi LLM dalam SOC ITS dapat diimplementasikan secara efektif, terdapat beberapa rekomendasi strategis yang perlu diperhatikan.

Pertama, perlu disiapkan infrastruktur komputasi yang mendukung, terutama jika menggunakan model LLM berskala besar.

Kedua, penting untuk menerapkan anonimisasi data dan kebijakan privasi yang ketat untuk melindungi data sensitif.

Ketiga, pelatihan SDM dalam penggunaan dan evaluasi sistem berbasis AI perlu dilakukan agar analis mampu bekerja secara kolaboratif dengan sistem.

Terakhir, sistem harus mendukung mechanism feedback loop dan memiliki audit log untuk evaluasi dan akuntabilitas.

Dengan memperhatikan aspek teknis, etis, dan operasional tersebut, SOC berbasis AI dapat menjadi solusi jangka panjang bagi pengelolaan ancaman siber di lingkungan pendidikan tinggi.

SIMPULAN

Penelitian ini menyimpulkan bahwa Security Operations Center (SOC) di lingkungan pendidikan tinggi seperti ITS menghadapi tantangan serius dalam proses deteksi dan triase insiden keamanan siber, khususnya karena tingginya volume alert, keterbatasan tenaga analis, serta kompleksitas sistem yang menghasilkan data log dalam jumlah besar. Untuk menjawab tantangan tersebut, pemanfaatan Large Language Models (LLM) seperti GPT-4 dan LLaMA 3 terbukti berpotensi meningkatkan efisiensi dan akurasi klasifikasi alert melalui kemampuan analisis kontekstual dan penyusunan penjelasan dalam bahasa alami.

Berdasarkan hasil studi literatur, dirancanglah kerangka sistem konseptual yang mengintegrasikan SIEM (Wazuh) dengan LLM Agent, dilengkapi dengan komponen filtering, pelaporan, dan feedback loop untuk mendukung proses triase yang lebih adaptif. Kerangka sistem ini dirancang untuk mengurangi beban kerja analis, mempercepat waktu respons, dan menjaga akurasi klasifikasi melalui pendekatan hybrid antara otomatisasi dan supervisi manusia.

Dengan dukungan strategi teknis dan kebijakan yang tepat, sistem ini dinilai layak untuk diterapkan di lingkungan SOC ITS maupun institusi pendidikan tinggi lainnya yang ingin mengembangkan sistem keamanan siber berbasis kecerdasan buatan.

SARAN

Berdasarkan kesimpulan tersebut, beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah:

1. Pengembangan tahap lanjut dapat dilakukan melalui implementasi simulasi sistem yang telah dirancang, menggunakan data log anonim dari SOC ITS sebagai studi kasus penerapan.
2. Institusi perlu mulai mempersiapkan kebijakan internal dan pelatihan SDM terkait pemanfaatan AI dalam keamanan siber, guna memastikan kesiapan operasional dan etis.
3. Evaluasi dan audit berkala perlu disusun untuk meminimalkan risiko kesalahan klasifikasi oleh model LLM, serta untuk mengembangkan sistem feedback yang adaptif terhadap perubahan pola serangan
4. Kolaborasi antara divisi IT, akademisi, dan lembaga eksternal seperti BSSN atau penyedia cloud security dapat menjadi langkah strategis dalam mendukung transformasi SOC berbasis AI di lingkungan perguruan tinggi.

REFERENSI

IBM Security, Cost of a Data Breach Report 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

J. Wang, T. Yan, D. An, Z. Liang, C. Guo, H. Hu, Q. Luo, H. Li, H. Wang, S. Zeng, C. Zhou, L. Ma, and F. Qi, “A comprehensive security operation center based on big data analytics and threat intelligence,” Proc. 2021 Int. Conf. on Cyber Security and Protection of Digital Services (Cyber Security), Oct. 2021. doi: 10.22323/1.378.0028.

N. Tziritas, P. Kikiras, S. Sanchez, and L. Iliadis, “The next generation cognitive security operations center: Adaptive analytic lambda architecture for efficient defense against adversarial attacks,” Big Data and Cognitive Computing, vol. 3, no. 1, p. 6, Jan. 2019. doi: 10.3390/bdcc3010006.

M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, and N. S. Thandi, “Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT/IIoT devices,” arXiv preprint arXiv:2306.14263, 2024. [Online]. Available: https://arxiv.org/abs/2306.14263.

P. Ranade, A. Piplai, A. Joshi, and T. Finin, “CyBERT: Contextualized embeddings for the cybersecurity domain,” in Proc. IEEE Int. Conf. on Big Data (Big Data), Dec. 2021, pp. 3334–3342. doi: 10.1109/BigData52589.2021.9671824.

Y. Singh, N. Patel, and S. K. Shandilya, “Enhancing Security Operations Center Efficiency through

Multi-Model Integration of Large Language Models and SIEM Systems," Research Square, Dec. 2024. doi: https://doi.org/10.21203/rs.3.rs-5615639/v1

Badan Siber dan Sandi Negara (BSSN), Laporan Tahunan 2023, [Online]. Available: https://www.cnbcindonesia.com/tech/20230712162824-37-453708/boho ng-internet-ri-aman-bssn-beberkan-buktinya

National Institute of Standards and Technology (NIST), "Computer Security Resource Center," 2020. [Online]. Available: https://csrc.nist.gov/

D. Parker, Managing Cybersecurity Operations Centers. Boca Raton, FL, USA: CRC Press, 2021.

What is SIEM", IBM, 2024. [Online]. Available: https://www.ibm.com/topics/siem

A. Johnson, K. Dempsey, R. Ross, S. Gupta, and D. Bailey, Guide for Security-Focused Configuration Management of Information Systems,

M. Cinque, D. Cotroneo, and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," in Proc. IEEE ISSRE Workshops,

A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in Advances in Neural Information Processing Systems (NeurIPS), vol. 30, 2017.

T. B. Brown et al., "Language Models are Few-Shot Learners," Advances in Neural Information Processing Systems, vol. 33, pp. 1877–1901, 2020. [Online]. Available: https://arxiv.org/abs/2005.14165

A. Radford et al., "Language Models are Unsupervised Multitask Learners," OpenAI, 2019. [Online]

I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016. [Online]. Available: https://www.deeplearningbook.org/