

State-of-the-Art Artificial Intelligence: Identifying Thesis Opportunities for MSIT Students

1. Introduction

Purpose: Artificial Intelligence (AI) is undergoing a period of unprecedented growth and transformation, impacting nearly every sector of the global economy and society. The continuous emergence of new State-of-the-Art (SOTA) models and techniques fuels this evolution, opening up vast possibilities for innovation and application.¹ This report aims to navigate this dynamic landscape to identify and analyze potential Master of Science in Information Technology (MSIT) thesis opportunities grounded in current SOTA AI research. The objective is to synthesize recent advancements and trends into actionable research directions suitable for a graduate student in IT.

Context: The analysis draws upon a curated collection of research findings covering diverse AI topics. These include advancements in Natural Language Processing (NLP), particularly for under-resourced languages like Indonesian³; the application of AI in enhancing government operations and consular services⁵; the role of AI in revolutionizing software development and cybersecurity⁷; and the critical, cross-cutting themes of SOTA models (e.g., Large Language Models (LLMs), Diffusion Models), techniques (e.g., Retrieval-Augmented Generation (RAG), Fine-tuning, Explainable AI (XAI)), and ethical considerations.¹

Target Audience and Scope: This report is specifically designed for an MSIT student seeking guidance on selecting a relevant and impactful thesis topic. The scope is focused on translating the findings from the provided research materials into concrete, feasible project ideas that align with the practical and applied nature of an MSIT program.

Roadmap: The report begins with an overview of the current AI landscape, highlighting key SOTA trends, models, and techniques. It then delves into specific potential thesis areas, detailing concrete project ideas derived from the research. Subsequently, it discusses crucial factors for selecting a thesis topic, including feasibility, novelty, impact, and ethical considerations. The report concludes with a summary table and recommendations to aid the student's decision-making process.

2. The Evolving AI Landscape (SOTA 2024-2025)

Overview: The field of AI is advancing at an extraordinary pace, marked by the frequent introduction of new SOTA models that push the boundaries of performance on established benchmarks.¹ This progress is not confined to traditional AI

strongholds like NLP and computer vision; it increasingly extends into specialized domains such as scientific discovery, healthcare, software engineering, and cybersecurity.² The transformative potential of AI is evident, driven by powerful architectures like the Transformer¹, massive datasets, and innovative training techniques.

Key Trends Shaping AI Research:

- **Efficiency and Accessibility:** A significant trend is the development of highly capable AI models that are considerably smaller and more efficient than their predecessors. For instance, models like Microsoft's Phi-3-mini demonstrate performance on par with much larger models from previous years on benchmarks like MMLU, achieved with drastically fewer parameters.¹³ This improvement in model optimization, coupled with a dramatic reduction in the cost of querying AI models (inference costs), is making advanced AI capabilities more accessible.¹³ Furthermore, the rise of powerful open-weight models, such as Meta's Llama series and Google's Gemma, is narrowing the performance gap compared to proprietary, closed-weight models.² This democratization is pivotal; the decreasing reliance on massive computational resources and proprietary access lowers the barrier to entry for researchers and students. Consequently, MSIT students, who may have limited access to extensive computational infrastructure compared to large industrial labs, can now realistically undertake thesis projects involving SOTA-level models and techniques previously considered out of reach.
- **Multimodality:** AI is moving beyond processing single data types (like text or images) towards systems that can understand, interpret, and generate information across multiple modalities. Models like OpenAI's GPT-4o and Google's Gemini can process combinations of text, images, audio, and video, enabling richer interactions and new applications.² This trend is evident in areas like visual question answering, text-to-video generation¹², and even multimodal threat detection in cybersecurity, where analyzing text, images, and code together provides a more comprehensive understanding.⁸
- **AI Agents and Reasoning:** There is a growing focus on creating AI agents – systems that can reason, plan, decompose tasks, and utilize tools (like web search or code execution) to achieve complex goals.² Frameworks such as LangChain, LangGraph, Microsoft's AutoGen, and CrewAI provide building blocks for developing these agents.²² These agents represent a shift from passive generation or prediction towards more autonomous problem-solving. Techniques like test-time compute, where models are allowed more processing time to iteratively refine their reasoning, have shown significant performance improvements on complex tasks, albeit sometimes at increased cost and latency.¹⁴

- **Responsible AI (RAI):** As AI becomes more powerful and pervasive, the importance of responsible development and deployment is paramount. This encompasses ethical considerations, fairness, transparency, accountability, privacy, and security.² The increasing number of documented AI-related incidents, from biased decision-making to the generation of harmful content, underscores this need.¹³ Consequently, there is a growing push for standardized RAI evaluations (e.g., HELM Safety, AIR-Bench²), Explainable AI (XAI) techniques to make model decisions transparent¹⁰, and regulatory frameworks to govern AI use, with significant activity observed globally and at the state level within the U.S..²

Dominant Models and Architectures:

- **Transformers:** The Transformer architecture, introduced in 2017, remains the cornerstone of many SOTA models.¹ Its parallel processing capabilities and attention mechanism have enabled unprecedented scaling and performance in both NLP (e.g., BERT, GPT families) and, more recently, Computer Vision (e.g., Vision Transformers or ViTs).¹ Models like BERT and its multilingual variants (mBERT, XLM-RoBERTa) are frequently used for tasks like question answering and text classification.²⁸
- **Large Language Models (LLMs):** LLMs such as OpenAI's GPT series (including GPT-4o, o3, o4-mini)¹⁶, Google's Gemini¹⁸, Meta's Llama¹⁵, Anthropic's Claude¹⁵, and Mistral³³ dominate the NLP landscape. They exhibit remarkable abilities in text generation, comprehension, translation, summarization, and increasingly, complex reasoning and coding.² Specialized LLMs are also emerging, tailored for specific domains like programming (e.g., CodeLlama) or languages, such as Sahabat AI for Indonesian and its dialects.³⁵
- **Diffusion Models:** These generative models have become the SOTA for high-fidelity image and video generation.¹ Models like Google's Imagen 3¹², Stability AI's Stable Diffusion variants¹⁴, OpenAI's Sora⁴⁰, and Google DeepMind's Veo 2¹² can create highly realistic and detailed visual content from text prompts or other inputs.
- **Graph Neural Networks (GNNs):** GNNs are designed to operate on graph-structured data, making them suitable for tasks involving relationships and connections, such as social network analysis, recommendation systems, molecular modeling⁴¹, and knowledge graph reasoning.⁴
- **Foundation Models:** This term refers to large models pre-trained on vast amounts of data, designed to be adaptable (often through fine-tuning) to a wide range of downstream tasks.¹ LLMs and large vision models are prominent examples of foundation models.

Emerging Techniques and Frameworks:

- **Retrieval-Augmented Generation (RAG):** RAG is a powerful technique that enhances LLM outputs by retrieving relevant information from an external knowledge source (like a database, document collection, or knowledge graph) before generating a response.³ This helps ground the LLM's generation in factual data, reducing hallucinations and improving relevance, particularly for domain-specific or knowledge-intensive tasks like question answering in Indonesian³ or providing up-to-date information. GraphRAG extends this by specifically leveraging knowledge graphs for retrieval.⁴²
- **Fine-tuning:** Adapting large pre-trained foundation models to specific tasks or domains remains a crucial step.²⁸ Full fine-tuning can be resource-intensive, leading to the development of Parameter-Efficient Fine-Tuning (PEFT) methods like LoRA (Low-Rank Adaptation) and its variants (e.g., QLoRA, which combines LoRA with quantization).⁴⁵ These techniques allow adaptation with significantly fewer trainable parameters, making fine-tuning more accessible.⁴⁷ Knowledge distillation, where a smaller "student" model learns from a larger "teacher" model, is another approach for creating efficient specialized models.⁴⁹
- **Reinforcement Learning from Human Feedback (RLHF) / Direct Preference Optimization (DPO):** These techniques are used to align LLM behavior with human preferences, making models more helpful, harmless, and honest.⁹ RLHF involves training a reward model based on human comparisons of model outputs, while DPO offers a more direct method for optimizing the LLM based on preference data.
- **Explainable AI (XAI):** As AI models become more complex ("black boxes"), techniques for explaining their predictions and decisions are critical.¹⁰ Methods like LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) provide insights into which input features influenced a model's output.²⁵ XAI is essential for building trust, debugging models, ensuring fairness, detecting biases, and meeting regulatory compliance requirements, especially in high-stakes domains like healthcare, finance, AIOps, and cybersecurity.²⁵
- **Agent Frameworks:** Frameworks like LangChain²², LangGraph²², AutoChain²³, Microsoft's AutoGen²², CrewAI²³, and AgentGPT²³ provide abstractions and tools to simplify the development of AI agents. They facilitate connecting LLMs to tools, managing memory and state, and orchestrating complex, multi-step workflows involving reasoning and planning.²⁰

3. Potential MSIT Thesis Opportunities

This section translates the SOTA AI landscape discussed above into specific, feasible thesis opportunities relevant to an MSIT program. The ideas leverage the provided research materials, focusing on applied research, system development, evaluation, and addressing identified challenges within specific domains.

Area 1: Applied NLP for Low-Resource Languages (Focus: Indonesian)

Context: The Indonesian language, despite having a large number of speakers, is considered relatively low-resource in terms of high-quality digital data and specialized NLP tools compared to languages like English.³ This presents challenges but also significant opportunities for applying SOTA AI techniques. Key challenges include data scarcity, linguistic diversity (including regional languages and code-switching), and the need for domain-specific information access (e.g., medical, historical, government services).³ Recent progress includes the development of Indonesian-specific models like IndoBERT⁵³ and Sahabat AI³⁵, as well as the application of techniques like RAG³ and efficient fine-tuning⁴⁷ to bridge the resource gap.

Idea 1.1: Enhancing Indonesian Question Answering with Advanced RAG Techniques

- **Description:** This thesis would investigate and compare the effectiveness of different Retrieval-Augmented Generation (RAG) strategies for improving Question Answering (QA) systems specifically for Indonesian. While standard RAG combines external document retrieval with LLM generation to improve factuality³, limitations like generic answers can persist.³³ This project could compare a baseline RAG approach against more advanced methods. One avenue is exploring GraphRAG, which leverages structured knowledge from Knowledge Graphs (KGs) during retrieval⁴², potentially addressing semantic gap issues noted in traditional ontology-based QA for Indonesian.⁴ Another direction could involve optimizing the retriever or generator components specifically for Indonesian linguistic characteristics or focusing on a particular domain like Indonesian medical herbs³³ or history⁴ where specialized knowledge is crucial.
- **Techniques/Models:** RAG, GraphRAG, LLMs (e.g., Llama 3 Sahabat AI³⁷, Mistral 7b³³, other multilingual models), Vector Databases (e.g., Faiss³³), Knowledge Graphs (e.g., built using Neo4j⁴² or domain ontologies⁴), Indonesian NLP models (e.g., IndoBERT⁵³).
- **Data/Tools:** Indonesian QA datasets (e.g., subset of TyDi QA²⁸), domain-specific Indonesian corpora (e.g., medical journals³³, historical texts⁴, government FAQs), RAG frameworks (e.g., LangChain²², LlamaIndex²³), HuggingFace Transformers library.²⁸
- **Evaluation:** Standard QA metrics such as F1 score, Exact Match (EM)⁵⁵, along

with metrics assessing generation quality like ROUGE³³ and METEOR.³³ Human evaluation for factual accuracy and relevance is also crucial.³³

- **Rationale:** The identified need for better Indonesian QA systems, stemming from data limitations and the shortcomings of both pure LLM generation and traditional ontology QA³, makes this a relevant problem. Comparing different RAG approaches, particularly the integration of structured knowledge via GraphRAG⁴², directly investigates potential solutions to overcome these limitations by providing more contextually relevant and factually accurate answers.

Idea 1.2: Efficient Fine-tuning of Pre-trained Models for Specialized Indonesian Domains

- **Description:** This project would focus on adapting large pre-trained language models (PLMs) for specific, potentially low-resource, Indonesian tasks or domains using efficient adaptation techniques. While large models like IndoBERT, XLM-RoBERTa, or Sahabat AI show strong performance on general Indonesian benchmarks³⁰, fully fine-tuning them for every niche task can be computationally prohibitive. This thesis would explore and evaluate methods like Parameter-Efficient Fine-Tuning (PEFT) – such as LoRA or QLoRA⁴⁵ – or knowledge distillation⁴⁹ to adapt these models effectively with lower resource requirements. Potential application domains could include sentiment analysis on Indonesian social media text exhibiting code-switching⁵³, classification of specific types of user inquiries (e.g., consular service requests), or abstractive summarization of Indonesian texts in specialized fields like medicine.⁴⁸
- **Techniques/Models:** PEFT (LoRA, QLoRA), Knowledge Distillation, Transfer Learning⁴⁸, Model Quantization⁴³, LLMs/Transformers (e.g., IndoBERT⁵³, XLM-R³⁰, Llama 3 Sahabat AI³⁵, T5⁴⁸).
- **Data/Tools:** Indonesian benchmark datasets (e.g., IndoNLU⁵³, NusaX⁵³), domain-specific Indonesian datasets (e.g., social media posts, medical abstracts, consular inquiries), HuggingFace libraries (Transformers, PEFT), relevant evaluation scripts.
- **Evaluation:** Task-specific performance metrics (e.g., accuracy, F1-score for classification; ROUGE, BLEU for generation/summarization³³), model size, inference speed, training time, and computational cost (e.g., GPU hours).
- **Rationale:** Large PLMs have proven effective for Indonesian⁵³, but applying them to diverse, specialized, and often low-resource tasks remains a challenge.⁴⁷ The SOTA trend towards efficient adaptation techniques⁴³ offers a practical solution. This thesis would involve applying and rigorously evaluating these techniques in the Indonesian context, assessing the trade-offs between model performance and computational efficiency, making advanced AI more practical for specific

Indonesian needs.

Idea 1.3: Developing and Evaluating an AI Chatbot for Indonesian Migrant Worker Support (SARI Case Study)

- **Description:** This thesis proposes building upon the Indonesian government's initiative for the Sahabat Artificial Migrant Indonesia (SARI) chatbot, designed to support Indonesian migrant workers (PMI).⁵⁶ The project would involve developing a prototype or enhancing a specific module of such a chatbot using SOTA technologies. Potential focus areas include: accurately answering questions about procedures (e.g., registration, document renewal) by retrieving information from official FAQs⁶¹; assisting with common problems reported by PMI⁶⁴; or implementing features for empathetic and gender-responsive communication, recognizing the specific challenges faced by female PMI.⁵⁹ A key component would be evaluating the chatbot's effectiveness through user feedback and performance metrics.
- **Techniques/Models:** Chatbot frameworks (e.g., Rasa, Google Dialogflow⁷⁰), LLMs (potentially Sahabat AI³⁵ or other suitable models), RAG (for accessing FAQs and procedural documents), Sentiment Analysis, Intent Recognition⁷¹, Multilingual capabilities (handling Indonesian and potentially regional dialects or English⁵²).
- **Data/Tools:** Official FAQs from relevant Indonesian government bodies (Ministry of Foreign Affairs - Kemlu, Agency for the Protection of Indonesian Migrant Workers - BP2MI)⁶¹, information from the Safe Travel application⁵⁸, potentially anonymized datasets of common PMI queries or problems⁶⁵, chatbot development platforms, evaluation methods including user studies⁸⁰ and automated metrics.⁸¹
- **Evaluation:** User experience evaluation through qualitative feedback and quantitative usability scores (e.g., Likert scales for ease of use, usefulness, satisfaction⁸⁰). Performance metrics like response accuracy, task completion rate, comprehension level, and self-service rate.⁸¹ Assessment of empathetic and gender-responsive aspects through user perception studies.
- **Rationale:** Migrant workers often face difficulties accessing timely and reliable information and support services.⁶⁴ The SARI initiative aims to address this using AI.⁵⁶ This thesis provides an opportunity to contribute to this real-world application with significant social impact by developing and evaluating a specific, functional component using SOTA chatbot technologies, grounded in the actual needs and data sources related to Indonesian migrant workers.

Area 2: AI for Enhanced Public/Citizen Services (Focus: Consular Domain)

Context: Governments globally are increasingly adopting AI to improve the efficiency and accessibility of public services, including consular assistance for citizens abroad.⁵ AI can automate routine tasks, provide instant information, and potentially personalize services.⁸⁵ However, implementation faces challenges such as handling diverse and multilingual inquiries, ensuring data privacy and security, integrating with existing government IT systems, and maintaining ethical standards like fairness and accountability.²⁴

Idea 2.1: Developing and Evaluating a Multilingual Consular FAQ Chatbot using LLMs and RAG

- **Description:** This project involves designing, building, and evaluating an AI-powered chatbot to automate responses to frequently asked questions (FAQs) related to consular services. Consulates handle a high volume of repetitive inquiries regarding passport renewals, visa applications, document legalization, emergency procedures, etc..⁸⁶ This chatbot would leverage a suitable LLM (potentially a multilingual model like XLM-R or mBERT³⁰, or a fine-tuned BERT²⁹) combined with RAG. The RAG component would retrieve accurate answers from official sources, such as embassy FAQ pages⁶¹ or government websites.¹⁰⁵ The chatbot should support multiple relevant languages (e.g., Indonesian and English for an Indonesian embassy, or German and English for a German embassy⁷¹). Evaluation would compare its performance against baseline information retrieval methods.
- **Techniques/Models:** LLMs (Multilingual models like XLM-R³⁰, mBERT⁷¹, or fine-tuned models like BERT²⁹), RAG, Vector Databases, Intent Recognition, Multilingual NLP techniques⁵², Chatbot Frameworks/APIs.⁷⁰
- **Data/Tools:** Official consular FAQ documents from various embassies/consulates (e.g., Indonesia⁶¹, Australia⁶², Saudi Arabia⁷⁵, Malaysia⁶¹, Netherlands⁷³, USA¹⁰¹), government websites (e.g., kemlu.go.id), potentially anonymized logs of common user queries, RAG frameworks (LangChain, LlamaIndex), HuggingFace library.
- **Evaluation:** Response accuracy (fact-checking against source documents), task completion rate for informational queries, user satisfaction surveys⁸⁰, robustness in handling out-of-scope or ambiguous questions, consistency of performance across supported languages.
- **Rationale:** Consular offices face significant workload from repetitive inquiries.⁸⁸ Automating FAQ responses with an accurate, multilingual chatbot, grounded in official information via RAG, directly addresses this operational challenge. This aligns with global trends in government AI adoption for citizen services⁵ and can free up consular staff for more complex cases requiring human judgment.⁸⁵ The

availability of structured FAQ data from embassy websites makes this feasible.

Idea 2.2: AI-driven User Segmentation for Personalized Consular Information Delivery

- **Description:** This thesis explores the application of AI-based user segmentation techniques, commonly used in marketing ¹¹³, to the domain of consular services. The goal is to develop and evaluate machine learning models (e.g., clustering algorithms like K-Means, or classification models) to group users of digital consular platforms (like Indonesia's Portal Peduli WNI ⁵⁸ or Safe Travel app ⁵⁸) based on their profiles, needs, and interaction patterns. These segments could differentiate between students, migrant workers, short-term tourists, long-term residents, etc. The derived segments would then inform the delivery of more personalized and relevant information, such as targeted safety alerts, reminders about visa expirations, or recommendations for specific consular services available through the platforms.
- **Techniques/Models:** Unsupervised Clustering (K-Means, DBSCAN), Supervised Classification (SVM, Random Forest, Neural Networks), Predictive Modeling (e.g., predicting likelihood of needing a specific service), User Behavior Analysis, AI Customer Segmentation principles. ¹¹³
- **Data/Tools:** Anonymized user interaction data from consular web portals or mobile apps (access and privacy considerations are paramount), user-provided profile information (e.g., residency status, purpose of stay), survey data on user needs, Python ML libraries (Scikit-learn, TensorFlow/PyTorch), potentially adapted Customer Data Platform (CDP) concepts.
- **Evaluation:** Quality of generated segments (e.g., using metrics like silhouette score for clustering), accuracy of classification/prediction models, and, importantly, the potential effectiveness of personalization based on these segments (e.g., simulated A/B testing of targeted messages, user feedback on relevance).
- **Rationale:** Digital platforms like Peduli WNI and Safe Travel aim to provide effective services and protection. ⁷⁶ However, users have diverse needs. Applying AI segmentation ¹¹³ can enhance the relevance and impact of information disseminated through these platforms, moving beyond one-size-fits-all communication towards proactive, personalized support tailored to different user groups (e.g., specific security advice for travelers vs. procedural information for residents). This addresses the challenge of effectively reaching diverse citizen populations abroad.

Idea 2.3: Framework for Integrating AI Chatbots into Existing Government

Service Platforms (e.g., Peduli WNI)

- **Description:** This thesis focuses on the practical IT challenges of integrating AI-powered components, such as chatbots, into existing government digital service platforms, using Indonesian consular platforms like Portal Peduli WNI or Safe Travel as a case study. The research would involve analyzing potential integration architectures and proposing a technical and operational framework. Key aspects to address include: ensuring seamless data synchronization between the chatbot and backend systems, designing robust and secure APIs for communication, managing security risks and ensuring compliance with data privacy regulations, planning for scalability to handle user load, and maintaining a consistent user experience across the integrated system.⁸⁵ The output could be a detailed framework document, potentially accompanied by a proof-of-concept integration demonstrating key aspects like secure API calls or data flow.
- **Techniques/Models:** Systems Integration principles, API Design (RESTful APIs, GraphQL), Microservices Architecture, Cloud Deployment strategies (AWS, Azure, Google Cloud ⁷¹), Data Security Protocols (Encryption, Authentication, Authorization, Access Control ⁷¹), DevOps and AIOps practices for deployment and monitoring.
- **Data/Tools:** Analysis of existing government platform architectures (based on public information or hypothetical scenarios), API documentation standards (e.g., OpenAPI), government IT security and privacy guidelines ²⁴, case studies of public sector IT modernization and integration projects.⁸⁵
- **Evaluation:** Feasibility analysis of the proposed framework, assessment of its security provisions, evaluation of its scalability potential, comparison with alternative integration approaches, clarity and completeness of the framework documentation.
- **Rationale:** Successfully deploying AI in government often hinges on overcoming the technical hurdles of integrating new technologies with complex, often legacy, IT systems.⁸⁵ As Indonesia develops multiple digital consular tools (Peduli WNI, Safe Travel, SARI ⁵⁶), effective integration becomes crucial. This thesis tackles these practical IT challenges, moving beyond AI model development to address real-world implementation, deployment, and operationalization – core competencies within an MSIT program.

Area 3: Advancing AI in Software Development & IT Operations (AIOps)

Context: AI is significantly impacting the software development lifecycle (SDLC) and IT operations (ITOps). AI-powered tools assist with code generation, automated testing, debugging, and even AI pair programming.⁷ In ITOps, AI (often termed AIOps)

is used for tasks like intelligent log analysis, anomaly detection, alert correlation, and automated incident response to manage increasingly complex IT environments.¹⁰ Key technologies include LLMs specialized for code, AI agent frameworks, and performance benchmarks like SWE-Bench.⁷ Ensuring the reliability and trustworthiness of these AI systems through Explainable AI (XAI) is also a growing concern.¹⁰

Idea 3.1: Benchmarking LLMs for Code Generation and Debugging on Domain-Specific Tasks

- **Description:** This thesis proposes a focused evaluation of various LLMs (e.g., OpenAI's GPT-4o¹⁶, Meta's Llama 3¹⁵, dedicated code models like CodeLlama, or other open-source alternatives) on specific, domain-relevant software development tasks. While general coding benchmarks like HumanEval and SWE-Bench exist¹⁴, performance can differ substantially when applied to specialized areas common in IT, such as developing applications using specific web frameworks (e.g., React, Angular), writing data analysis scripts using libraries like Pandas/NumPy, or debugging code within particular enterprise software environments. The project would involve creating custom test suites or adapting existing benchmarks to reflect these specific domains, evaluating model performance not just on correctness but potentially also on code quality, efficiency, and security¹¹⁸, and analyzing the effectiveness of different prompting strategies.
- **Techniques/Models:** LLMs for Code Generation/Debugging (GPT-4o, Llama 3, CodeLlama, etc.), Prompt Engineering, Automated Software Testing Frameworks (e.g., Pytest, JUnit, Selenium), Static Code Analysis tools.
- **Data/Tools:** Code repositories (e.g., GitHub, internal enterprise codebases if accessible and anonymized), existing coding benchmarks (HumanEval, MBPP, SWE-Bench¹⁴), custom-developed coding problems and test cases, LLM APIs or locally hosted open-source models, HuggingFace library.
- **Evaluation:** Code correctness (pass rate on functional tests), code quality metrics (e.g., cyclomatic complexity, adherence to style guides), code efficiency (e.g., execution time), vulnerability scanning results (using tools like SonarQube or Snyk), comparison of different models and prompting techniques.
- **Rationale:** General coding benchmarks provide valuable but incomplete information about an LLM's utility for specific, practical software engineering tasks encountered in industry.¹⁴ Evaluating models on domain-specific benchmarks provides more actionable insights for developers and organizations deciding which tools to adopt. This aligns well with the applied focus of an MSIT

program, offering practical relevance beyond theoretical benchmark scores.

Idea 3.2: Building and Evaluating AI Agents for Automated AIOps Tasks

- **Description:** This project focuses on leveraging the emerging capabilities of AI agents² for automating complex tasks within IT Operations (AIOps). Using frameworks like LangChain, AutoGen, or CrewAI²², the thesis would involve developing an AI agent designed to handle a specific AIOps workflow. Examples include: analyzing streams of system logs to perform root cause analysis of incidents; correlating alerts from disparate monitoring tools (e.g., network, application, infrastructure) to reduce alert fatigue; automatically generating draft incident reports summarizing key events and findings; or proposing remediation actions based on historical incident data and documented procedures accessed via RAG. The evaluation would focus on the agent's accuracy, efficiency, and impact on reducing manual operator effort.
- **Techniques/Models:** AI Agent Architectures, LLMs (for reasoning and text generation), RAG (to access knowledge bases, runbooks, log data), Log Parsing algorithms, Anomaly Detection models, Time Series Analysis, Planning and Tool Use capabilities within agent frameworks.
- **Data/Tools:** Real or simulated system logs (e.g., syslog, application logs, Kubernetes logs), monitoring system data/alerts (e.g., from Prometheus, Zabbix, Datadog), incident tickets/data (e.g., from ServiceNow, Jira), IT documentation/knowledge bases, Agent Development Frameworks (LangChain, AutoGen, etc.), LLM APIs.
- **Evaluation:** Accuracy of the agent's output (e.g., correctness of root cause identification, relevance of suggested remediation), speed of task completion compared to manual methods, reduction in alert noise or mean time to resolution (MTTR), qualitative feedback from IT operators on the agent's usefulness.
- **Rationale:** Managing modern IT infrastructure generates vast amounts of data, making manual analysis and response challenging.¹⁰ AIOps aims to apply AI to automate and improve these processes.¹⁰ AI agents, with their ability to reason, plan, and use tools²⁰, represent a significant advancement in automation potential beyond simple scripting. This thesis applies this SOTA agent technology to solve practical AIOps problems, directly relevant to IT management and operations.

Idea 3.3: Applying Explainable AI (XAI) Techniques to AI Models in Software Engineering or AIOps

- **Description:** This thesis focuses on enhancing the transparency and trustworthiness of AI models used in software engineering or AIOps domains. The

project would involve selecting a relevant AI model (e.g., a model predicting software defects, an LLM used for code completion, an anomaly detection model for system logs, an alert correlation engine) and applying various XAI techniques to interpret its behavior. Techniques like LIME, SHAP, Integrated Gradients, or attention mechanism visualization could be employed.²⁵ The core of the thesis would be evaluating the quality and utility of the generated explanations from the perspective of the target users (software developers or IT operators). This evaluation could assess whether the explanations increase trust, aid in debugging the AI model itself, help identify potential biases in the model's decisions, or lead to improved human-AI collaboration in the respective tasks.

- **Techniques/Models:** XAI methods (LIME, SHAP, Integrated Gradients, Attention Visualization, etc.), target AI models used in SE/AIOps (e.g., Recurrent Neural Networks (RNNs)/LSTMs for sequential log data, Transformer models for code, Convolutional Neural Networks (CNNs) for performance data visualization, traditional ML models like Random Forests).
- **Data/Tools:** Datasets used to train the chosen AI model (e.g., code repositories, commit histories, system logs, performance metrics), XAI libraries (e.g., SHAP library, LIME library, Captum for PyTorch), visualization libraries (Matplotlib, Seaborn, specialized XAI visualization tools).
- **Evaluation:** Qualitative user studies involving software developers or IT operators to assess the clarity, usefulness, and trustworthiness of the explanations. Quantitative analysis could involve measuring how explanations impact task performance (e.g., speed or accuracy of debugging a faulty AI prediction). Comparison of the insights provided by different XAI techniques for the specific application.
- **Rationale:** As AI takes on more critical roles in software development and IT operations, understanding *why* these systems make certain predictions or recommendations is crucial for adoption, debugging, and ensuring responsible use.¹⁰ Applying XAI addresses the "black box" problem inherent in many complex models. This thesis provides a practical investigation into the value of XAI within the IT domain, evaluating how well different techniques bridge the gap between AI decisions and human understanding for developers and operators.

Area 4: Multimodal AI for Cybersecurity

Context: The cybersecurity landscape is increasingly complex, with adversaries employing sophisticated tactics that often blend different types of data. Phishing attacks may combine deceptive text with fake logos or website screenshots; malware might be embedded within seemingly benign multimedia files or use visual elements to evade detection.⁸ Multimodal AI, capable of jointly analyzing data from different

sources (text, images, code, network traffic, etc.), offers a powerful approach to combat these evolving threats.⁸ Evaluating the effectiveness¹⁹ and ensuring the trustworthiness (via XAI⁵⁰) of these multimodal security systems are key research areas.

Idea 4.1: Developing a Multimodal Phishing Detection System using Text and Visual Analysis

- **Description:** This thesis aims to design, implement, and evaluate a phishing detection system that leverages both textual and visual cues. Traditional phishing detection often focuses solely on text content or URL analysis. However, modern attacks frequently use sophisticated visual mimicry (e.g., replicating login pages, using legitimate-looking logos).⁸ This project would develop a system that integrates NLP models (e.g., BERT, LLMs) to analyze email text (subject, body, sender) for suspicious language patterns and social engineering tactics, with computer vision models (e.g., ViT, CNNs) to analyze embedded images, logos, or screenshots of linked websites for visual inconsistencies or signs of forgery. Feature fusion techniques would combine insights from both modalities for a final classification decision. The system's performance would be benchmarked against unimodal (text-only or image-only) approaches.
- **Techniques/Models:** Multimodal AI architectures, LLMs (e.g., BERT, RoBERTa, fine-tuned LLMs), Vision Models (ViT, ResNet, EfficientNet), Feature Fusion methods (e.g., concatenation, cross-attention), Classification algorithms (e.g., SVM, Logistic Regression, Neural Networks). Models with inherent multimodal capabilities like GPT-4o could also be explored.⁸
- **Data/Tools:** Publicly available phishing datasets that include both email text and visual elements (e.g., from PhishTank, APWG, academic research datasets) or potentially custom-collected datasets. Python libraries for NLP (HuggingFace Transformers), Computer Vision (PyTorch Vision, TensorFlow Hub, OpenCV), and Machine Learning (Scikit-learn). Optical Character Recognition (OCR) tools might be needed for extracting text from images.
- **Evaluation:** Standard classification metrics (Accuracy, Precision, Recall, F1-score, AUC-ROC). Crucially, evaluation should include performance against sophisticated attacks (e.g., zero-day phishing kits, attacks using novel visual deception) and comparison with unimodal baselines to demonstrate the value of the multimodal approach.⁸
- **Rationale:** Phishing remains a prevalent and costly cybersecurity threat.⁴⁵ As attackers increasingly use visual elements to enhance deception⁸, detection methods must evolve. This thesis directly addresses this challenge by applying SOTA multimodal AI techniques⁸ to analyze both text and image data

concurrently, aiming for more robust detection than traditional methods relying on a single modality.

Idea 4.2: Evaluating Multimodal AI Models on Emerging Cybersecurity Benchmarks

- **Description:** This project involves a systematic evaluation of the capabilities of recent SOTA multimodal foundation models (e.g., OpenAI's GPT-4V/GPT-4o, Google's Gemini Pro Vision, open-source models like LLaVA) specifically on cybersecurity-related tasks. While these models demonstrate impressive general multimodal understanding, their effectiveness and reliability for specific security applications need rigorous assessment. The thesis would involve selecting or adapting relevant benchmarks that incorporate multimodal data relevant to cybersecurity. Potential tasks could include: classifying malware based on both its disassembled code (text) and its runtime behavior visualized as images or graphs; analyzing cyber threat intelligence reports that contain text, diagrams, and network graphs; or assessing software vulnerabilities based on code snippets combined with architectural diagrams. The evaluation should focus on comparing different models, identifying their strengths, weaknesses, and potential failure modes in the security context.
- **Techniques/Models:** Multimodal LLMs/Foundation Models (GPT-4V/o, Gemini Vision, LLaVA, etc.), Benchmarking frameworks and methodologies, Performance evaluation metrics.
- **Data/Tools:** Existing cybersecurity datasets that can be adapted for multimodal evaluation (e.g., malware repositories with associated behavior reports, threat intelligence feeds), potentially using benchmarks like Priv-IQ¹⁹ or methodologies inspired by security leaderboards like CalypsoAI.¹²² Model APIs (OpenAI, Google AI Studio/Vertex AI) or locally hosted open-source models.
- **Evaluation:** Task-specific metrics (e.g., classification accuracy, F1-score, vulnerability detection rate), robustness analysis (e.g., performance under noisy or adversarial inputs), computational cost (latency, throughput), qualitative analysis of model outputs and error types.
- **Rationale:** The rapid emergence of powerful multimodal foundation models presents new opportunities for cybersecurity.⁸ However, their actual utility and reliability for specific, high-stakes security tasks are not yet well understood. Standardized benchmarking is crucial.¹⁹ This thesis addresses this gap by performing a comparative evaluation of leading multimodal models on cybersecurity-specific tasks, providing valuable insights for practitioners and researchers on the practical applicability and limitations of these SOTA models in

the security domain.

Idea 4.3: Applying Explainable AI (XAI) to Multimodal Threat Detection Systems

- **Description:** This thesis combines the advancements in multimodal AI for cybersecurity with the critical need for explainability. The project would involve taking a multimodal threat detection system (such as the phishing detector from Idea 4.1, or a system classifying malware using multiple data types) and applying XAI techniques to make its decision-making process transparent and interpretable to human analysts. The challenge lies in developing or adapting XAI methods that can effectively attribute the model's prediction to features across different modalities – for example, highlighting which specific words in an email *and* which specific visual elements in an attached image contributed most strongly to classifying it as phishing. The evaluation would focus on the quality of these cross-modal explanations and their usefulness for security professionals in understanding, trusting, and potentially overriding the AI's judgment.
- **Techniques/Models:** XAI methods suitable for multimodal architectures (e.g., attention map visualization, gradient-based attribution methods like Integrated Gradients applied across modalities, model-agnostic methods like LIME or SHAP adapted for multimodal feature spaces), the target Multimodal AI model for threat detection.
- **Data/Tools:** The dataset used to train and test the multimodal threat detection model (e.g., multimodal phishing dataset, malware dataset with multiple feature types), XAI libraries (SHAP, LIME, Captum, etc.), visualization tools capable of highlighting features in both text and images/graphs.
- **Evaluation:** Assessing the faithfulness (how accurately explanations reflect the model's reasoning) and plausibility (how convincing explanations are to humans) of the generated explanations, potentially through user studies with security analysts. Evaluating the impact of explanations on analyst trust, decision-making speed/accuracy, and ability to identify model errors. Comparing different XAI techniques for their effectiveness in the multimodal security context.
- **Rationale:** While multimodal AI promises enhanced threat detection⁸, the complexity of these models makes them potential "black boxes," hindering trust and adoption by security analysts who need to understand the reasoning behind alerts.⁵⁰ Applying XAI to these systems⁵⁰ is crucial for building trust, enabling effective human-AI collaboration, and ensuring accountability. This thesis tackles the cutting-edge challenge of achieving explainability in complex, multimodal systems within the critical domain of cybersecurity.

4. Considerations for Thesis Selection

Choosing an appropriate MSIT thesis topic requires careful consideration of several factors beyond just the technical interest. The following points should guide the selection process:

- **Feasibility:**

- **Data Availability:** This is often a critical bottleneck. Assess whether the required datasets are publicly available (e.g., benchmark datasets like IndoNLU⁵³, TyDi QA²⁸, SWE-Bench¹¹⁹), obtainable through partnerships, scrapable from the web, or need to be generated (e.g., synthetic data¹²¹). Research involving low-resource languages⁴ or highly specific domains (like internal AIOps logs or sensitive consular data) may require significant effort in data collection, annotation, or anonymization. Access to government or enterprise data often involves navigating privacy and security protocols.
- **Computational Resources:** Training or fine-tuning large AI models (LLMs, diffusion models) can be computationally expensive. While the trend towards smaller, efficient models¹³ and PEFT techniques⁴⁵ alleviates this burden, significant tasks might still require access to GPUs or cloud computing resources (e.g., Google Colab, university clusters, AWS/Azure/GCP⁷¹). Evaluate the resource requirements of the chosen models and techniques against available resources.
- **Scope Management:** A common pitfall in research is defining a scope that is too broad. It is crucial to formulate a specific, answerable research question and define clear, achievable objectives within the timeframe of a Master's thesis. Avoid trying to solve *all* problems in a domain. Focus on a specific comparison, evaluation, application, or technique. Employing structured approaches to define requirements and manage scope, potentially inspired by frameworks like NEDF for system building¹²³, can prevent scope drift and ensure timely completion. Narrowing the focus is essential for success.¹²³

- **Novelty and Impact:**

- An MSIT thesis should aim to make a meaningful contribution. While groundbreaking theoretical discoveries might be beyond scope, novelty can be achieved in various ways: applying existing SOTA techniques to a new domain or dataset (e.g., GraphRAG for Indonesian medical QA); comparing different SOTA approaches in a specific context (e.g., benchmarking LLMs for a niche coding task); adapting techniques to address specific constraints (e.g., PEFT for low-resource Indonesian summarization); developing and evaluating a system addressing a real-world problem identified in the

literature (e.g., the SARI chatbot module); or creating a new benchmark or evaluation methodology for an emerging area (e.g., multimodal cybersecurity evaluation).

- Consider the potential impact of the research. Will it provide practical benefits to a specific community (e.g., Indonesian migrant workers, consular staff, software developers)? Will it contribute valuable insights or data to the research community? Aligning the project with identified needs or gaps in the literature strengthens its potential impact.

- **Relevance to MSIT:**

- The thesis topic should align with the core principles and learning objectives of an Information Technology program. While involving AI/ML, the project should ideally incorporate aspects of system design, implementation, data management, network considerations, security practices, platform integration, performance evaluation, or IT operations (AIOps). Projects that are purely theoretical machine learning explorations might be less suitable than those involving the application, integration, or evaluation of AI within an IT context. Ideas like the AI integration framework (2.3), the AIOps agent (3.2), or the development and evaluation of user-facing systems like chatbots (1.3, 2.1) demonstrate strong IT relevance.

- **Ethical Considerations:**

- Responsible AI practices must be integrated throughout the thesis process. This involves critically assessing datasets and models for potential biases (e.g., gender, linguistic, socioeconomic) and implementing mitigation strategies where possible.²
- Data privacy is paramount, especially when dealing with user data, government information, or sensitive domains like healthcare or cybersecurity.¹⁹ Ensure compliance with relevant regulations (e.g., GDPR²⁷) and employ techniques like anonymization or differential privacy if necessary.¹²¹
- Strive for transparency and accountability in the research process and in the AI systems developed. Utilizing XAI techniques¹⁰ can contribute to this. Adhere to ethical guidelines, such as those proposed by UNESCO.²⁴
- Consider the potential societal impacts and risks of misuse associated with the developed technology.⁵

5. Conclusion and Recommendations

Summary: The current AI landscape presents a wealth of opportunities for impactful MSIT thesis research. Key SOTA trends, including the rise of efficient and accessible

models, the shift towards multimodality, the development of sophisticated AI agents, and the increasing emphasis on Responsible AI, are opening new avenues for exploration. This report has synthesized these trends with specific research findings to propose concrete thesis ideas across several relevant domains: enhancing NLP for low-resource languages like Indonesian, applying AI to improve public and consular services, advancing AI's role in software development and IT operations, and leveraging multimodal AI for cybersecurity.

Synthesis Table: The following table summarizes the potential thesis opportunities discussed, highlighting key aspects to aid in selection.

Table 1: Summary of Potential MSIT Thesis Opportunities

Area	Thesis Idea Title	Key Techniques/Models	Potential Data/Tools	Feasibility Notes (Data/Compute/Scope)
Applied NLP - Indonesian	Enhancing Indonesian QA with Advanced RAG	RAG, GraphRAG, LLMs (Sahabat AI), KG, Vector DB	TyDi QA (Indo), Domain Corpora (Medical/History), LangChain/LlamaIndex	Data: Med-High, Compute: Med, Scope: High (Needs focus)
Applied NLP - Indonesian	Efficient Fine-tuning for Specialized Indonesian Domains	PEFT (LoRA/QLoRA), Distillation, IndoBERT, XLM-R, Sahabat AI	IndoNLU/NusaX, Domain Datasets (Social Media/Medical), HuggingFace PEFT	Data: Med, Compute: Low-Med, Scope: Med
Applied NLP - Indonesian	Developing/Evaluating AI Chatbot for Migrant Worker Support (SARI)	Chatbots, LLMs (Sahabat AI), RAG, Sentiment Analysis	Gov FAQs (Kemlu/BP2MI), Safe Travel Info, User Queries (Anonymized), Chatbot Platforms, User Studies	Data: Med, Compute: Low-Med, Scope: Med
AI for Public/Consular	Multilingual Consular FAQ	LLMs (Multilingual/BE	Embassy FAQs (Various), Gov	Data: Med, Compute: Med,

r Services	Chatbot using LLMs and RAG	RT), RAG, Intent Recognition	Websites, LangChain/LlamaIndex, Chatbot Frameworks	Scope: Med
AI for Public/Consular Services	AI-driven User Segmentation for Personalized Consular Info	Clustering, Classification, Predictive Models, User Analysis	Anonymized Platform Data (Peduli WNI/Safe Travel), User Profiles, Surveys, Python ML Libs	Data: High (Access/Privacy), Compute: Low, Scope: Med
AI for Public/Consular Services	Framework for Integrating AI Chatbots into Gov Service Platforms	Systems Integration, APIs, Cloud Deployment, Security	Platform Analysis, API Docs, Gov IT Standards, Case Studies	Data: Low (Conceptual), Compute: Low, Scope: Med-High
AI for SE/AIOps	Benchmarking LLMs for Domain-Specific Code Gen/Debugging	LLMs for Code, Prompting, Automated Testing	Code Repos, SWE-Bench (Adapted), Custom Code Datasets, LLM APIs	Data: Med, Compute: Med, Scope: Med
AI for SE/AIOps	Building/Evaluating AI Agents for Automated AIOps Tasks	AI Agents, LLMs, RAG, Log Analysis, Anomaly Detection	System Logs, Monitoring Data, Incident Data, Agent Frameworks (LangChain/AutoGen)	Data: Med-High (Access/Simulation), Compute: Med, Scope: Med
AI for SE/AIOps	Applying XAI to AI Models in Software Engineering or AIOps	XAI (LIME, SHAP), Target AI Models (RNN/Transformer/CNN)	Model Training Data (Code/Logs/Metrics), XAI Libraries (SHAP/LIME), User Studies	Data: Med, Compute: Low-Med, Scope: Med
Multimodal AI - Cybersecurity	Multimodal Phishing	Multimodal AI, LLMs, Vision	Multimodal Phishing	Data: Med, Compute: Med,

	Detection (Text + Visual)	Models (ViT/CNN), Fusion	Datasets, NLP/CV Libraries (HuggingFace, PyTorch/TF)	Scope: Med
Multimodal AI - Cybersecurity	Evaluating Multimodal AI Models on Cybersecurity Benchmarks	Multimodal LLMs (GPT-4V/Gemini), Benchmarking	Cybersecurity Datasets (Multimodal), Security Benchmarks (e.g., Priv-IQ, CalypsoAI-inspired), Model APIs/Libraries	Data: Med-High, Compute: Med-High, Scope: Med
Multimodal AI - Cybersecurity	Applying XAI to Multimodal Threat Detection Systems	XAI for Multimodal, Attention/Gradient Methods	Multimodal Threat Datasets, XAI Libraries, Visualization Tools, User Studies	Data: Med, Compute: Med, Scope: Med-High


Recommendations for Student:

1. **Align with Interests and Strengths:** Reflect on which AI areas (NLP, agents, cybersecurity, etc.) and application domains (Indonesian context, public services, IT operations) resonate most strongly with personal interests and existing technical skills.
2. **Conduct Deeper Literature Review:** Select 1-2 thesis ideas from the table that seem most promising and conduct a more focused literature review to understand the specific SOTA within that narrow area, identify precise research gaps, and refine the research question.
3. **Consult Faculty Advisors:** Discuss the shortlisted ideas with potential faculty advisors. Their expertise is invaluable for assessing the feasibility within the program's constraints, gauging the novelty, refining the scope, and identifying available resources (data, compute, software).
4. **Prioritize Feasibility:** Be realistic about data accessibility and computational requirements. Choose a topic where the necessary resources are likely to be available or can be reasonably acquired/simulated. Start with a well-defined, manageable scope.
5. **Embed Ethical Considerations:** Regardless of the chosen topic, proactively

consider and address ethical implications related to data privacy, bias, fairness, transparency, and potential misuse from the outset of the project.

Concluding Thought: The intersection of State-of-the-Art AI and Information Technology offers fertile ground for exciting and impactful Master's thesis research. By carefully considering the trends, opportunities, and practical constraints outlined in this report, MSIT students can identify and pursue projects that not only contribute to the field but also provide valuable skills and experiences for their future careers.

Works cited

1. State-of-the-Art (SOTA) AI Models: LLMs, NLP, and Computer Vision - Automatio, accessed May 8, 2025, <https://automatio.ai/blog/sota-models-llm-nlp/>
2. The 2025 AI Index Report | Stanford HAI, accessed May 8, 2025, <https://hai.stanford.edu/ai-index/2025-ai-index-report>
3. UTILIZING RETRIEVAL-AUGMENTED GENERATION IN LARGE LANGUAGE MODELS TO ENHANCE INDONESIAN LANGUAGE NLP - EJournal Universitas Nusa Mandiri, accessed May 8, 2025, <https://ejournal.nusamandiri.ac.id/index.php/jitk/article/download/5916/1292>
4. Indonesian Linguistic Ontology for Enhancing Ontology-Based Indonesian Question-Answering Systems | Request PDF - ResearchGate, accessed May 8, 2025, https://www.researchgate.net/publication/388694434_Indonesian_Linguistic_Ontology_for_Enhancing_Ontology-Based_Indonesian_Question-Answering_Systems
5. AI in government: Top use cases - IBM, accessed May 8, 2025, <https://www.ibm.com/think/topics/ai-in-government>
6. AI Embassies: A New Frontier in Cyber Domain - Journal of Cyberspace Studies, accessed May 8, 2025, https://jcass.ut.ac.ir/article_100581_e88fa4dcea93291e80233e66497e581e.pdf
7. Sibayaktoto  Login Situs Toto 4d dan Agen Togel Dana 4d ..., accessed May 8, 2025, <https://ijcsrr.org/artificial-intelligence-in-software-development-a-review-of-code-generation-testing-maintenance-and-security/>
8. The sixth sense for cyber defense: Multimodal AI – Sophos News, accessed May 8, 2025, <https://news.sophos.com/en-us/2025/03/19/the-sixth-sense-for-cyber-defense-multimodal-ai/>
9. Deep Learning 2025: Federated, Reinforcement, Transfer - SoluLab, accessed May 8, 2025, <https://www.solulab.com/ai-deep-learning-techniques/>
10. www.ust.com, accessed May 8, 2025, [https://www.ust.com/en/insights/the-imperative-for-explainable-ai-in-aiops#:~:text=Explainable%20AI%20\(XAI\)%20refers%20to,the%20advice%20AI%20Ops%20tools%20provide.](https://www.ust.com/en/insights/the-imperative-for-explainable-ai-in-aiops#:~:text=Explainable%20AI%20(XAI)%20refers%20to,the%20advice%20AI%20Ops%20tools%20provide.)
11. AI Conference Deadlines, accessed May 8, 2025, <https://aideadlin.es/>

12. 2024: A year of extraordinary progress and advancement in AI - Google Blog, accessed May 8, 2025, <https://blog.google/technology/ai/2024-ai-extraordinary-progress-advancement/>
13. AI Index 2025: State of AI in 10 Charts | Stanford HAI, accessed May 8, 2025, <https://hai.stanford.edu/news/ai-index-2025-state-of-ai-in-10-charts>
14. Technical Performance | The 2025 AI Index Report | Stanford HAI, accessed May 8, 2025, <https://hai.stanford.edu/ai-index/2025-ai-index-report/technical-performance>
15. Key Takeaways from State of AI Report 2024 and 2025 Predictions - Learn Prompting, accessed May 8, 2025, <https://learnprompting.org/blog/state-of-AI-report-2024>
16. Model Release Notes | OpenAI Help Center, accessed May 8, 2025, <https://help.openai.com/en/articles/9624314-model-release-notes>
17. Introducing OpenAI o3 and o4-mini, accessed May 8, 2025, <https://openai.com/index/introducing-o3-and-o4-mini/>
18. Google DeepMind, accessed May 8, 2025, <https://deepmind.google/>
19. Priv-IQ: A Benchmark and Comparative Evaluation of Large ... - MDPI, accessed May 8, 2025, <https://www.mdpi.com/2673-2688/6/2/29>
20. 1st International Workshop (2025) on AI Agent Reasoning and Decision-Making, accessed May 8, 2025, <https://ai-agent-reasoning.com/>
21. AI Agents! Giving Reasoning and Tools to LLMs - Context & Code Examples - YouTube, accessed May 8, 2025, <https://www.youtube.com/watch?v=GZWFLjOUqI>
22. 25 LangChain Alternatives You MUST Consider In 2025 - Akka, accessed May 8, 2025, <https://akka.io/blog/langchain-alternatives>
23. Top 10 LangChain Alternatives for AI Workflows in 2025 - Openxcell, accessed May 8, 2025, <https://www.openxcell.com/blog/langchain-alternatives/>
24. Ethics of Artificial Intelligence | UNESCO, accessed May 8, 2025, <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
25. What is Explainable AI (XAI)? - ServiceNow, accessed May 8, 2025, <https://www.servicenow.com/au/ai/what-is-explainable-ai.html>
26. Global Trends in AI Governance - World Bank Documents and Reports, accessed May 8, 2025, <https://documents1.worldbank.org/curated/en/099120224205026271/pdf/P1786161ad76ca0ae1ba3b1558ca4ff88ba.pdf>
27. Ethical and Responsible AI Adoption in Government - REI Systems, accessed May 8, 2025, <https://www.reisystems.com/roadmap-to-transformation-the-next-generation-of-government-operations-with-ethical-and-responsible-ai-adoption/>
28. A Fine-Tuned BART Pre-trained Language Model for the Indonesian Question-Answering Task, accessed May 8, 2025, <https://etasr.com/index.php/ETASR/article/download/9828/4742/45262>
29. BERT Question Answering System - Grid Dynamics, accessed May 8, 2025, <https://www.griddynamics.com/blog/question-answering-system-using-bert>
30. FacebookAI/xlm-roberta-large - Hugging Face, accessed May 8, 2025,

- <https://huggingface.co/FacebookAI/xlm-roberta-large>
31. Multilingual Propaganda Detection: Exploring Transformer-Based Models mBERT, XLM-RoBERTa, and mT5 - ACL Anthology, accessed May 8, 2025, <https://aclanthology.org/2025.nakbanlp-1.9.pdf>
 32. The latest AI news we announced in April - Google Blog, accessed May 8, 2025, <https://blog.google/technology/ai/google-ai-updates-april-2025/>
 33. Integrating Retrieval-Augmented Generation with Large Language Model Mistral 7b for Indonesian Medical Herb - ResearchGate, accessed May 8, 2025, https://www.researchgate.net/publication/384328184_Integrating_Retrieval-Augmented_Generation_with_Large_Language_Model_Mistral_7b_for_Indonesian_Medical_Herb
 34. LLM Security: Vulnerabilities, Attacks, Defenses, and Countermeasures - arXiv, accessed May 8, 2025, <https://arxiv.org/html/2505.01177v1>
 35. Sahabat AI: The Friend Indonesia Needs for a Digital Future - Twimbit, accessed May 8, 2025, <https://twimbit.com/about/blogs/sahabat-ai-the-friend-indonesia-needs-for-a-digital-future>
 36. Sahabat-AI, accessed May 8, 2025, <https://sahabat-ai.com/>
 37. GoToCompany/llama3-8b-cpt-sahabatai-v1-instruct - Hugging Face, accessed May 8, 2025, <https://huggingface.co/GoToCompany/llama3-8b-cpt-sahabatai-v1-instruct>
 38. NeurIPS 2024 Accepted Paper List - Paper Copilot, accessed May 8, 2025, <https://papercopilot.com/paper-list/neurips-paper-list/neurips-2024-paper-list/>
 39. CVPR 2024 Papers, accessed May 8, 2025, <https://cvpr.thecvf.com/virtual/2024/papers.html>
 40. How Far Are We From AGI? - arXiv, accessed May 8, 2025, <https://arxiv.org/html/2405.10313v1>
 41. [NeurIPS 2024] LLaMo: Large Language Model-based Molecular Graph Assistant, accessed May 8, 2025, <https://www.youtube.com/watch?v=IRhJkI3FFiE>
 42. Building, Improving, and Deploying Knowledge Graph RAG Systems on Databricks, accessed May 8, 2025, <https://www.databricks.com/blog/building-improving-and-deploying-knowledge-graph-rag-systems-databricks>
 43. [P] I created a package implementing a SOTA technique for XAI (Explainable AI) - Reddit, accessed May 8, 2025, https://www.reddit.com/r/MachineLearning/comments/1666yyn/p_i_created_a_package_implementing_a_sota/
 44. Question Answering with a Fine-Tuned BERT - Chris McCormick, accessed May 8, 2025, <https://mccormickml.com/2020/03/10/question-answering-with-a-fine-tuned-BERT/>
 45. Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities - arXiv, accessed May 8, 2025, <https://arxiv.org/html/2405.12750v2>
 46. (PDF) Generative AI in Cybersecurity: A Comprehensive Review of LLM

- Applications and Vulnerabilities - ResearchGate, accessed May 8, 2025,
https://www.researchgate.net/publication/388632472_Generative_AI_in_Cybersecurity_A_Comprehensive_Review_of_LLM_Applications_and_Vulnerabilities
47. Fine-Tuning Small Language Models for Indonesian Languages, Trivan Menezes, UG '25 (19115) - Princeton Media Central, accessed May 8, 2025,
https://mediacentral.princeton.edu/media/Fine-Tuning+Small+Language+Models+for+Indonesian+Languages%2C+Trivan+Menezes%2C+UG+25+%2819115%29/1_nil56g8g
 48. Towards Two-Step Fine-Tuned Abstractive Summarization for Low-Resource Language Using Transformer T5 - The Science and Information (SAI) Organization, accessed May 8, 2025,
<https://thesai.org/Publications/ViewPaper?Volume=16&Issue=2&Code=IJACSA&SerialNo=120>
 49. Accepted Findings Papers - ACL 2024, accessed May 8, 2025,
https://2024.aclweb.org/program/finding_papers/
 50. (PDF) Explainable AI (XAI) in Cybersecurity: Bridging the Gap ..., accessed May 8, 2025,
https://www.researchgate.net/publication/390113611_Explainable_AI_XAI_in_Cybersecurity_Bridging_the_Gap_Between_AI_and_Human_Understanding/download
 51. www.researchgate.net, accessed May 8, 2025,
[https://www.researchgate.net/publication/390113611_Explainable_AI_XAI_in_Cybersecurity_Bridging_the_Gap_Between_AI_and_Human_Understanding#:~:text=Explainable%20AI%20\(XAI\)%20has%20emerged,intelligence%2C%20and%20ensures%20regulatory%20compliance.](https://www.researchgate.net/publication/390113611_Explainable_AI_XAI_in_Cybersecurity_Bridging_the_Gap_Between_AI_and_Human_Understanding#:~:text=Explainable%20AI%20(XAI)%20has%20emerged,intelligence%2C%20and%20ensures%20regulatory%20compliance.)
 52. Multilingual NLP Made Simple [Challenges, Solutions & The Future], accessed May 8, 2025,
<https://spotintelligence.com/2023/09/19/multilingual-nlp-made-simple-challenges-solutions-the-future/>
 53. arXiv:2403.01817v1 [cs.CL] 4 Mar 2024, accessed May 8, 2025,
<https://arxiv.org/pdf/2403.01817>
 54. NusaBERT: Teaching IndoBERT to be Multilingual and Multicultural - arXiv, accessed May 8, 2025, <https://arxiv.org/html/2403.01817v1>
 55. A Fine-Tuned BART Pre-trained Language Model for the Indonesian Question-Answering Task | Engineering, Technology & Applied Science Research, accessed May 8, 2025, <https://etasr.com/index.php/ETASR/article/view/9828>
 56. Aplikasi chatbot SARI lengkapi celah informasi bagi PMI di luar negeri - Antaranews, accessed May 8, 2025,
<https://www.antaranews.com/berita/4784749/aplikasi-chatbot-sari-lengkapi-celah-informasi-bagi-pmi-di-luar-negeri>
 57. Wamen P2MI Apresiasi Peluncuran SARI, Chatbot untuk Lindungi Pekerja Migran Indonesia, accessed May 8, 2025,
<https://planet.merdeka.com/hot-news/wamen-p2mi-apresiasi-peluncuran-sari-chatbot-untuk-lindungi-pekerja-migran-indonesia-381696-mvk.html>
 58. Foreign Ministry to Utilize AI-Based Services for Indonesian Citizens ..., accessed May 8, 2025,

- <https://en.tempo.co/read/1975389/foreign-ministry-to-utilize-ai-based-services-for-indonesian-citizens-abroad>
59. Bantu Pekerja Migran, Wamen Christina Apresiasi ... - BP2MI, accessed May 8, 2025,
<https://www.bp2mi.go.id/berita-detail/bantu-pekerja-migran-wamen-christina-apresiasi-peluncuran-fitur-chatbot-sari-dari-kemlu>
 60. Migration MPTF Final Report, accessed May 8, 2025,
https://mptf.undp.org/sites/default/files/documents/2025-02/final_report_2024_migration_mptf_indonesia.pdf
 61. Pelayanan Kependidikan KBRI Kuala Lumpur (Legalisir Ijazah, Surat Pindah Sekolah, dll), accessed May 8, 2025, <https://kemlu.go.id/kualalumpur/faq>
 62. Ketentuan Barang Pindahan - Official Website Direktorat Jenderal Bea dan Cukai, accessed May 8, 2025,
<https://www.beacukai.go.id/faq/ketentuan-barang-pindahan.html>
 63. FAQ - Johor Bahru, accessed May 8, 2025, <https://kemlu.go.id/johorbahru/faq>
 64. Syarat Pelaporan Peristiwa Penting WNI di Luar Negeri, Cek Infonya! - detikNews, accessed May 8, 2025,
<https://news.detik.com/berita/d-7746189/syarat-pelaporan-peristiwa-penting-wni-di-luar-negeri-cek-infonya>
 65. Pelayanan dan Pelindungan WNI di Luar Negeri - Peduli WNI - Kemenlu, accessed May 8, 2025, <https://www.peduliwni.kemlu.go.id/pengaduan/form.html>
 66. Indonesian Ministerial Regulation to Protect Indonesian Citizens Abroad (No. 4/2008) - Migrants in Countries in Crisis (MICIC), accessed May 8, 2025,
<https://micicinitiative.iom.int/indonesian-ministerial-regulation-protect-indonesian-citizens-abroad-no-4/2008-0>
 67. Kemlu RI-UN Women Luncurkan SARI, asisten virtual untuk lindungi PMI - Fokus Taiwan, accessed May 8, 2025,
<https://indonesia.focustaiwan.tw/society/202504215001>
 68. Kemlu RI dan UN Women Luncurkan Chatbot SARI, Inovasi AI untuk Pelindungan Perempuan Pekerja Migran - Global Liputan6.com, accessed May 8, 2025,
<https://www.liputan6.com/global/read/6001356/kemlu-ri-dan-un-women-luncurkan-chatbot-sari-inovasi-ai-untuk-pelindungan-perempuan-pekerja-migran>
 69. Kemlu RI dan UN Women Perkuat Pelindungan Perempuan Pekerja Migran melalui Inovasi Chatbot AI SARI - NOA.co.id, accessed May 8, 2025,
<https://www.noa.co.id/kemlu-ri-dan-un-women-perkuat-pelindungan-perempuan-pekerja-migran-melalui-inovasi-chatbot-ai-sari/>
 70. 20 Best Chatbot APIs for Websites in 2025 (Free AI Integrations & Docs) - Copilot.Live, accessed May 8, 2025,
<https://www.copilot.live/blog/best-ai-chatbot-apis>
 71. Lucky-akash321/Building-Chatbot-using-BERT-LLM-for ... - GitHub, accessed May 8, 2025,
<https://github.com/Lucky-akash321/Building-Chatbot-using-BERT-LLM-for-German-Embassy>
 72. Kemlu Sebut Aplikasi SARI Lengkapi Informasi bagi Pekerja Migran - RRI, accessed May 8, 2025,

<https://www.rri.co.id/pusat-pemberitaan/nasional/1464772/kemlu-sebut-aplikasi-sari-lengkapi-informasi-bagi-pekerja-migran>

73. FAQ - Kedutaan Besar Republik Indonesia Den Haag, Belanda, accessed May 8, 2025, <https://indonesia.nl/faq/>
74. FAQ - Sydney, accessed May 8, 2025, <https://kemlu.go.id/sydney/faq>
75. FAQ - Riyadh, accessed May 8, 2025, <https://kemlu.go.id/riyadh/faq>
76. Diplomasi Digital dan Implementasi Aplikasi Safe Travel di Kementerian Luar Negeri Republik Indonesia, accessed May 8, 2025, <https://pesirah.ejournal.unsri.ac.id/index.php/jap/article/download/1/28/230>
77. Safe Travel - Apps on Google Play, accessed May 8, 2025, <https://play.google.com/store/apps/details?id=id.go.kemlu.safetravel>
78. Privacy Policy - Safe Travel, accessed May 8, 2025, <https://bo-safetravel.kemlu.go.id/privacy-policy>
79. Kemlu Perkuat Infrastruktur Hukum dalam Selesaikan Masalah WNI di Luar Negeri, accessed May 8, 2025, <https://www.hukumonline.com/berita/a/kemlu-perkuat-infrastruktur-hukum-dalam-selesaikan-masalah-wni-di-luar-negeri-lt66f201dc033e8/>
80. Evaluating User Experience With a Chatbot Designed as a Public Health Response to the COVID-19 Pandemic in Brazil: Mixed Methods Study, accessed May 8, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10131797/>
81. Measuring Chatbot Effectiveness: 16 KPIs to Track - Visiativ, accessed May 8, 2025, <https://www.visiativ.com/en/actualites/news/measuring-chatbot-effectiveness/>
82. peranan hubungan diplomatik dalam perlindungan warga negara indonesia di luar negeri, accessed May 8, 2025, <https://www.jurnal.poltekim.ac.id/jikk/article/download/573/496/>
83. Applications of artificial intelligence in global diplomacy: A review of research and practical models - ResearchGate, accessed May 8, 2025, https://www.researchgate.net/publication/390329776_Applications_of_artificial_intelligence_in_global_diplomacy_A_review_of_research_and_practical_models
84. How Governments are Using AI: 8 Real-World Case Studies, accessed May 8, 2025, <https://blog.govnet.co.uk/technology/ai-in-government-case-studies>
85. AI Solutions for Government: Transforming Public Sector Services - Zealous System, accessed May 8, 2025, <https://www.zealousys.com/blog/ai-solutions-for-government/>
86. Government Chatbots | AI-Powered Citizen Support & Services - Conversation Design Institute, accessed May 8, 2025, <https://www.conversationdesigninstitute.com/use-cases/government>
87. Economic and Social Council - United Nations Digital Library System, accessed May 8, 2025, https://digitallibrary.un.org/record/4079896/files/E_C.16_2025_4-EN.pdf
88. Improving the Visa Processing System at Department of State | United States Digital Service, accessed May 8, 2025, <https://www.usds.gov/report-to-congress/2016/visa-processing/>
89. AI in Government: A Strategic Framework for Digital Transformation - REI

- Systems, accessed May 8, 2025,
<https://www.reisystems.com/ai-in-government-a-strategic-framework-for-digital-transformation/>
90. Toward Meaningful Transparency and Accountability of AI Algorithms in Public Service Delivery - DAI, accessed May 8, 2025,
<https://www.dai.com/uploads/ai-in-public-service.pdf>
 91. Full article: Holding AI-Based Systems Accountable in the Public Sector: A Systematic Review - Taylor & Francis Online, accessed May 8, 2025,
<https://www.tandfonline.com/doi/full/10.1080/15309576.2025.2469784?src=exp-la>
 92. Navigating Governmental Choices: A Comprehensive Review of Artificial Intelligence's Impact on Decision-Making - MDPI, accessed May 8, 2025,
<https://www.mdpi.com/2227-9709/11/3/64>
 93. Challenges in Chatbot Development - SmythOS, accessed May 8, 2025,
<https://smythos.com/ai-agents/chatbots/challenges-in-chatbot-development/>
 94. GAO-25-108069, Priority Open Recommendations: Department of State, accessed May 8, 2025, <https://www.gao.gov/assets/gao-25-108069.pdf>
 95. Integrating Artificial Intelligence into Public Administration - MDPI, accessed May 8, 2025, <https://www.mdpi.com/2076-3387/15/4/149>
 96. AI Governance and Ethics: Lessons from the U.S. Visa Revocation Policy, accessed May 8, 2025,
<https://moderndiplomacy.eu/2025/03/11/ai-governance-and-ethics-lessons-from-the-u-s-visa-revocation-policy/>
 97. Artificial Intelligence in Diplomacy: Transforming Global Relations and Negotiations, accessed May 8, 2025,
<https://trendsresearch.org/insight/artificial-intelligence-in-diplomacy-transforming-global-relations-and-negotiations/>
 98. Indonesia International Travel Information, accessed May 8, 2025,
<https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages/Indonesia.html>
 99. Inspection of Embassy Jakarta and Constituent Post, Indonesia; ISP-I-25-01 - Department of State OIG, accessed May 8, 2025,
https://www.stateoig.gov/uploads/report/report_pdf_file/inspection-embassy-jakarta-and-constituent-posts-indonesia-isp-i-25-01.pdf
 100. www.mdpi.com, accessed May 8, 2025,
<https://www.mdpi.com/2076-3387/15/4/149#:~:text=Addressing%20challenges%20such%20as%20algorithmic.values%20and%20the%20public's%20trust.>
 101. Laporan Diri - Smart Consulate Office (SCO) KJRI New York, accessed May 8, 2025, <https://kjrinewyork.org/self-report>
 102. Pertanyaan yang sering ditanyakan(FAQ) - e-Consular Service KBRI WDC, accessed May 8, 2025, <https://consular.embassyofindonesia.org/page/wnifaq.html>
 103. KEDUTAAN BESAR REPUBLIK INDONESIA Riyadh, Kerajaan Saudi Arabia - Portal Kemlu, accessed May 8, 2025,
<https://fe-non-production.apps.opppd2-dev.layanan.go.id/perwakilan/d1fe173d08e959397adf34b1d77e88d7?type=perwakilan-detail>
 104. Layanan WNI - The Embassy of The Republic of Indonesia in Berlin, accessed

- May 8, 2025, <https://indonesianembassy.de/layanan-wni/>
105. Kementerian Luar Negeri RI - Portal Kemlu, accessed May 8, 2025, <https://fe-non-production.apps.opppd2-dev.layanan.go.id/kontak>
 106. the-ogre/finetuning_bert_for_qa: This project focuses on fine-tuning a BERT model for question answering using a limited dataset for illustration purposes. - GitHub, accessed May 8, 2025, <https://github.com/the-ogre/LLM-FinetuningBERTforQuestionAnswering>
 107. FAQs - Bert®, accessed May 8, 2025, <https://bertbrain.com/faqs/>
 108. What Is Extractive Question Answering? - Ontotext, accessed May 8, 2025, <https://www.ontotext.com/knowledgehub/fundamentals/what-is-extractive-question-answering/>
 109. Which Type of Language Service Provider Should I Choose? - Terra Translations, accessed May 8, 2025, <https://terratranslations.com/2019/07/24/type-of-language-service-provider-should-i-choose/>
 110. Conversational AI API | Find the Top API Solutions - aiOla, accessed May 8, 2025, <https://aiola.ai/blog/conversational-ai-apis/>
 111. Chatbots in the Public Sector: How AI-Driven Chatbots are ..., accessed May 8, 2025, <https://www.fxmweb.com/insights/chatbots-in-the-public-sector-how-ai-driven-chatbots-are-reshaping-government-services.html>
 112. Diplomacy in the Age of Artificial Intelligence, accessed May 8, 2025, <https://uscpublicdiplomacy.org/printpdf/89581>
 113. How to Use AI for Customer Segmentation? 5 Easy Steps & Insights - CleverTap, accessed May 8, 2025, <https://clevertap.com/blog/ai-customer-segmentation/>
 114. Unlock the Power of AI Customer Segmentation with AWS Marketplace - Amazon.com, accessed May 8, 2025, <https://aws.amazon.com/marketplace/solutions/generative-ai/what-is/ai-customer-segmentation/>
 115. Standar Pelayanan - Peduli WNI, accessed May 8, 2025, <https://peduliwni.kemlu.go.id/server-file/download/referensi/standarpelayanan.pdf.html>
 116. Peduli WNI - Kemenlu, accessed May 8, 2025, <https://peduliwni.kemlu.go.id/>
 117. Multilingual Chatbot: Benefits, Challenges & How to Build | WotNot, accessed May 8, 2025, <https://wotnot.io/blog/multilingual-chatbot>
 118. From Vulnerabilities to Remediation: A Systematic Literature Review of LLMs in Code Security - arXiv, accessed May 8, 2025, <https://arxiv.org/html/2412.15004v3>
 119. Amazon introduces SWE-PolyBench, a multilingual benchmark for ..., accessed May 8, 2025, <https://aws.amazon.com/blogs/devops/amazon-introduces-swe-polybench-a-multilingual-benchmark-for-ai-coding-agents/>
 120. Malicious Use of Multimodal AI Will Create Entire Attack Chains | 2025 Cybersecurity Predictions - YouTube, accessed May 8, 2025, <https://www.youtube.com/watch?v=OOjtlnnj8mw>

121. Generative AI-Enhanced Cybersecurity Framework for Enterprise ..., accessed May 8, 2025, <https://www.mdpi.com/2073-431X/14/2/55>
122. AI Security Leaderboard Reveals Model Cybersecurity - RTInsights, accessed May 8, 2025, <https://www.rtinsights.com/ai-security-leaderboard-reveals-model-cybersecurity/>
123. NLP for Project Documentation: Ensuring Clear Requirements to Avoid Scope Drift, accessed May 8, 2025, https://www.researchgate.net/publication/390303105_NLP_for_Project_Documentation_Ensuring_Clear_Requirements_to_Avoid_Scope_Drift
124. Natural Language Processing Technologies for Public Health in Africa: Scoping Review, accessed May 8, 2025, <https://pubmed.ncbi.nlm.nih.gov/40053738/>
125. AI Ethics in Public Policy: Case Studies & Challenges | ISPP, accessed May 8, 2025, <https://www.ispp.org.in/ethics-of-ai-in-public-policy-in-the-indian-context/>