# INTISARI

## RANCANG BANGUN APLIKASI BERBASIS LARGE LANGUAGE MODEL (TIRITH COPILOT) UNTUK MEMBANTU PEMBUATAN POLICY TIRITH

Oleh:
Rafid Aslam
20/464402/SV/18721

StackGuardian BV telah mengembangkan *policy engine* bernama Tirith secara *open-source*. *Policy engine* ini, pada umumnya, ditunjukkan untuk mencegah miskonfigurasi *cloud* yang umum terjadi di kalangan pengguna IaC (*Infrastructure as Code*). Definisi *policy* Tirith berupa JSON yang mudah untuk dibaca dan dimengerti. Namun, proses pembuatan *policy* sering kali dirasa sulit. Hal ini karena pembuat *policy* perlu untuk membuka dokumentasi tambahan di luar dokumentasi *Tirith* itu sendiri, seperti dokumentasi Terraform. Semakin banyak dokumentasi yang perlu untuk dibuka, semakin panjang prosesnya. *Large Language Model* (LLM) merupakan model *generative machine learning* yang dapat membuat kalimat dan susunan kata. LLM mempermudah proses pembuatan kode dan pencarian informasi. Hal ini karena LLM dapat menerima perintah dengan bahasa natural manusia. Lalu, menjawab perintah tersebut dengan hal yang diminta, misal seperti kode, kalimat, puisi, dan sebagainya. Penelitian tentang LLM sedang berada pada puncaknya dalam tiga tahun terakhir. Salah satu pemanfaatan LLM adalah pembuatan agen LLM. Agen LLM merupakan agen yang dapat menentukan sendiri langkah apa yang akan dilakukan selanjutnya untuk menyelesaikan permintaan pengguna. Penelitian ini membahas tentang bagaimana cara untuk menyelesaikan masalah pembuatan *policy* Tirith yang kompleks dengan agen LLM. Agen LLM dibungkus dalam aplikasi yang ramah pengguna yang dapat diakses melalui *browser*. Aplikasi diuji dengan tiga metode, yaitu LLM-as-a-judge, *load testing*, dan juga UAT. Evaluasi agen LLM menunjukkan bahwa agen dapat membuat *policy* Tirith dengan akurasi yang lebih tinggi dibandingkan menggunakan LLM biasa. Hasil *load testing* menunjukkan aplikasi dapat merespons dengan waktu rata-rata 11 detik. Aplikasi yang dikembangkan mencapai skor UAT 95,67%. Aplikasi ini ditujukan untuk pengguna *platform* StackGuardian untuk mempermudah pembuatan *policy* Tirtih.

Kata kunci: *Large Language Model*, *autonomous agent*, *policy engine*, LangChain

# *ABSTRACT*

## *DESIGN AND DEVELOPMENT OF A LARGE LANGUAGE MODEL BASED (TIRITH COPILOT) APPLICATION TO ASSIST TIRITH POLICY CREATION*

Rafid Aslam
20/464402/SV/18721

*StackGuardian BV has developed an open-source policy engine called Tirith. This policy engine is generally aimed at preventing common cloud misconfigurations often encountered by Infrastructure as Code (IaC) users. Tirith policy definitions are in JSON format, making them easy to read and understand. However, the policy creation process is often challenging, as policy creators need to refer to additional documentation outside of Tirith's own documentation, such as Terraform documentation. The more documentation required, the longer the process takes. A Large Language Model (LLM) is a generative machine learning model capable of generating text and word structures. LLMs simplify coding and information retrieval processes by accepting commands in natural human language and providing responses based on the request, such as code, sentences, poems, etc. Research on LLMs has reached its peak in the past three years. One application of LLMs is the development of LLM-based autonomous agents. These agents can independently determine the next steps to fulfill user requests. This study discusses how to solve the complex problem of Tirith policy creation using an LLM-based autonomous agent. The autonomous agent is packaged into a user-friendly application accessible via a web browser. The application is evaluated using three methods: LLM-as-a-judge, load testing, and User Acceptance Testing (UAT). The evaluation results show that the autonomous agent can create Tirith policies with higher accuracy compared to using a standard LLM. Load testing results indicate that the application responds with an average time of 11 seconds. The developed application achieved a UAT score of 95.67%. This application is intended to be used by StackGuardian platform's users to make the Tirith policy creation process easier.*

*Keywords: Large Language Model, autonomous agent, policy engine,* LangChain