INTISARI

Teknologi *blockchain* terus berkembang secara pesat dan banyak digunakan di berbagai sektor perindustrian. Namun, implementasi *blockchain* melalui *smart contract* masih menghadapi tantangan terkait celah keamanan. Lazimnya sebelum suatu proyek *blockchain* diterapkan, diperlukan audit keamanan *smart contract*. Beberapa penelitian sebelumnya telah mengeksplorasi kemampuan *Large Language Model* (LLM) untuk melakukan audit keamanan *smart contract* secara otomatis. Namun, penelitian-penelitian tersebut masih menggunakan LLM *closed-source* seperti GPT milik OpenAI ataupun LLM dengan jumlah parameter model yang besar. Hal ini menimbulkan dua kendala utama yaitu resiko privasi karena data harus dikirim ke pihak ketiga dan kebutuhan komputasi yang tinggi. Oleh karena itu, penelitian tugas akhir ini mengusulkan pemanfaatan LLM *open-source* dengan jumlah parameter model yang rendah untuk melakukan audit keamanan *smart contract* secara otomatis. Metode yang diusulkan membagi proses audit keamanan menjadi empat bagian yaitu deteksi kerentanan *smart contract*, penjelasan kerentanan *smart contract*, penentuan tingkat keparahan kerentanan dan rekomendasi penutupan celah keamanan *smart contract*. Tiap bagian proses audit keamanan ini selanjutnya ditugaskan ke tiap agen berbasis LLM dengan jumlah parameter model yang rendah. Pada tugas deteksi kerentanan, Agen Deteksi berhasil mencapai nilai metrik evaluasi yang merata sebesar 0,88, mengungguli CodeLlama-13B (0,87). Agen Penjelasan Kerentanan mencapai keselarasan dengan penjelasan manusia sebesar 25,17%, melebihi GPT-4o dan Codellama. Pada klasifikasi tingkat keparahan, Agen *Severity* berhasil mencapai nilai macro-average F1-score 0,64, Recall 0,63, dan Akurasi 0,66, tertinggi dibandingkan model *baseline* termasuk GPT-4o dan CodeLlama. Sementara itu, Agen Rekomendator meraih keselarasan rekomendasi tertinggi sebesar 53,15%, mengungguli *Finetuned-CodeLlama-13B* (50,35%) dan GPT-4o (32,87%). Hasil penelitian menunjukkan bahwa proses audit keamanan *smart contract* dapat dilakukan oleh siapapun bahkan oleh pihak yang memiliki keterbatasan sumber daya untuk menjalankan LLM. Selain itu, penelitian ini turut menjawab permasalahan privasi karena proses audit keamanan *smart contract* otomatis tidak lagi bergantung pada LLM *closed-source* sehingga memungkinkan pelaksanaan audit secara lokal tanpa mengirimkan data ke pihak ketiga.

Kata kunci : model bahasa besar, *lightweight*, *smart contract*, keamanan, *blockchain*

ABSTRACT

Blockchain technology continues to develop rapidly and is widely used in various industrial sectors. However, the implementation of blockchain through smart contracts still faces challenges related to security gaps. Typically, before a blockchain project is implemented, a smart contract security audit is required. Several previous studies have explored the ability of the Large Language Model (LLM) to automatically perform smart contract security audits. However, these studies still use closed-source LLMs such as OpenAI's GPT or LLMs with a large number of model parameters. This poses two main obstacles: the risk of privacy because data must be sent to third parties and high computational requirements. Therefore, this paper proposes utilizing an open-source LLM with a low number of model parameters to automatically audit the security of smart contracts. The proposed method divides the security audit process into four parts: smart contract vulnerability detection, smart contract vulnerability explanation, vulnerability severity determination and smart contract security gap closure recommendation. Each part of the security audit process was then assigned to each LLM-based agent with a low number of model parameters. On the vulnerability detection task, the Detection Agent achieved an aligned evaluation metric value of 0.88, outperforming CodeLlama-13B (0.87). The Vulnerability Explanation Agent achieved an alignment with human explanations of 25.17%, outperforming GPT-4o and Codellama. In severity classification, the Severity Agent achieved a macro-average F1-score of 0.64, Recall of 0.63, and Accuracy of 0.66, the highest compared to baseline models including GPT-4o and CodeLlama. Meanwhile, the Recommender Agent achieved the highest recommendation alignment of 53.15%, outperforming Finetuned-CodeLlama-13B (50.35%) and GPT-4o (32.87%). The results show that the smart contract security audit process can be done by anyone, even by who has limited resources to run LLM. In addition, this research also addresses privacy issues because the automated smart contract security audit process no longer relies on closed-source LLMs, allowing the audit to be conducted locally without sending data to third parties.

Keywords : *large language model*, *lightweight*, *smart contract*, *security*, *blockchain*