Implementasi dan Perbandingan Kinerja Pipeline DevSecOps Berbasis GitLab CI/CD dengan Integrasi
Blockchain Hyperledger Besu dan Nethermind
Ibnu Rasyid, Dr. Ir. Ronald Adrian, S.T., M.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

IMPLEMENTASI DAN PERBANDINGAN KINERJA *PIPELINE* DEVSECOPS BERBASIS GITLAB CI/CD DENGAN INTEGRASI *BLOCKCHAIN* HYPERLEDGER BESU DAN NETHERMIND

Ibnu Rasyid
22/495055/SV/20947

Peningkatan ancaman siber mendorong kebutuhan integrasi keamanan ke dalam siklus pengembangan perangkat lunak melalui pendekatan DevSecOps, sementara kebutuhan audit trail yang tidak dapat diubah (*immutable*) atas hasil pemindaian keamanan turut mendorong eksplorasi integrasi teknologi *blockchain* ke dalam *pipeline* CI/CD. Penelitian sebelumnya belum secara komprehensif mengevaluasi konfigurasi *pipeline* DevSecOps yang optimal dengan mempertimbangkan efisiensi eksekusi pada konfigurasi *runner* berbeda, performa jaringan *blockchain* sebagai media pencatatan *hash*, serta efektivitas integrasi analisis keamanan statis dan dinamis secara bersamaan. Penelitian ini mengimplementasikan *pipeline* DevSecOps berbasis GitLab CI/CD yang mengintegrasikan Semgrep, *Open Worldwide Application Security Project* (OWASP) ZAP, Trivy, serta pencatatan *hash* artefak melalui transaksi *blockchain* pada Nethermind (Clique PoA) dan Hyperledger Besu (QBFT), diuji pada konfigurasi *single worker* dan *multi worker* terhadap aplikasi OWASP Juice Shop. Hasil pengujian menunjukkan bahwa penggunaan *multi worker* mempercepat waktu eksekusi pipeline sebesar 8,57% dibandingkan *single worker*. Nethermind menunjukkan keandalan yang lebih rendah dibandingkan Hyperledger Besu, dengan *break point* atau titik jenuh sistem masing-masing pada 250 dan 500 pengguna konkuren. Selain itu, SAST dan DAST terbukti saling melengkapi dalam memperluas cakupan deteksi kerentanan. Penelitian selanjutnya diharapkan mengeksplorasi mekanisme konsensus *blockchain* lain serta lingkungan pengujian dengan sumber daya lebih memadai.

Kata Kunci: *Blockchain*, CI/CD, DevSecOps, Hyperledger Besu, Nethermind

UNIVERSITAS
GADJAH MADA
**Implementasi dan Perbandingan Kinerja Pipeline DevSecOps Berbasis GitLab CI/CD dengan Integrasi
Blockchain Hyperledger Besu dan Nethermind**
Ibnu Rasyid, Dr. Ir. Ronald Adrian, S.T., M.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

IMPLEMENTATION AND PERFORMANCE COMPARISON OF A GITLAB CI/CD-BASED DEVSECOPS PIPELINE WITH HYPERLEDGER BESU AND NETHERMIND BLOCKCHAIN INTEGRATION

Ibnu Rasyid
22/495055/SV/20947

The increasing prevalence of cyber threats has driven the need to integrate security practices into the software development lifecycle through the DevSecOps approach, while the need for an immutable audit trail of security scan results has further motivated the exploration of blockchain technology integration into CI/CD pipelines. Previous research has not comprehensively evaluated the optimal DevSecOps pipeline configuration by simultaneously considering execution efficiency across different runner configurations, blockchain network performance as a hash-recording medium, and the effectiveness of integrating static and dynamic security analysis. This research implements a GitLab CI/CD-based DevSecOps pipeline that integrates Semgrep, Open Worldwide Application Security Project (OWASP) ZAP, and Trivy, along with artifact hash recording through blockchain transactions on Nethermind (Clique PoA) and Hyperledger Besu (QBFT), tested under single worker and multi worker configurations against the OWASP Juice Shop application. The test results show that using multi worker accelerates pipeline execution time by 8.57% compared to single worker. Nethermind demonstrated lower reliability than Hyperledger Besu, with system breakpoints or saturation points at 250 and 500 concurrent users, respectively. Furthermore, SAST and DAST are shown to complement each other in extending vulnerability detection coverage. Future research is expected to explore alternative blockchain consensus mechanisms as well as testing environments with more adequate computational resources.

Keywords: *Blockchain*, CI/CD, DevSecOps, Hyperledger Besu, Nethermind