Meningkatkan Keamanan Data Genomik di Cloud melalui Enkripsi Homomorfik

Putrie Risky Khairunnisa[1], Muhamad Irsan, S.T., M.Kom., Ph.D.[2], Ikke Dian Oktaviani, S.Kom., M.Kom.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]putrriesky@students.telkomuniversity.ac.id, [2]irsanfaiz@telkomuniversity.ac.id, [3]idoktaviani@telkomuniversity.ac.id

Abstract

Genomic data contains highly sensitive genetic information, posing significant challenges in cloud computing security. Genomic information, being immutable and directly linked to personal identity, increases the risk of breaches such as identity theft, genetic discrimination, and unauthorized surveillance. Incidents like the MyHeritage data breach and unauthorized access to the GEDmatch database highlight these vulnerabilities. With the growing use of cloud computing for genomic data storage and processing, additional risks emerge due to third-party involvement and large-scale operations. This study adopts Homomorphic Encryption to secure genomic data without decryption, addressing privacy challenges while enabling secure computations in the cloud. Two encryption algorithms, RSA and Paillier, were evaluated based on execution time, throughput, and memory usage. The results indicate that RSA excels in execution time and throughput, while Paillier is more efficient in memory usage and supports secure computations directly on encrypted data. The proposed hybrid RSA-Paillier scheme offers a balanced framework for genomic data security, aligning with GDPR and HIPAA regulations and ensuring scalability in real-world cloud-based applications.

Keywords: Homomorphic Encryption, RSA, Paillier, Cryptography, Genomic data, Cloud computing