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

Abstrak

Data genomik mengandung informasi genetik yang sangat sensitif, sehingga menghadirkan tantangan besar dalam keamanan komputasi awan. Informasi genomik yang bersifat tidak dapat diubah dan terkait langsung dengan identitas pribadi meningkatkan risiko pelanggaran seperti pencurian identitas, diskriminasi genetik, dan pengawasan tanpa izin. Insiden seperti kebocoran data MyHeritage dan akses tidak sah ke basis data GEDmatch menggarisbawahi kerentanan ini. Dengan meningkatnya penggunaan komputasi awan untuk penyimpanan dan pemrosesan data genomik, risiko tambahan muncul akibat keterlibatan pihak ketiga dan operasi skala besar. Penelitian ini mengadopsi Enkripsi Homomorfik untuk mengamankan data genomik tanpa mendekripsinya, menjawab tantangan privasi sekaligus memungkinkan komputasi aman di cloud. Dua algoritma enkripsi, RSA dan Paillier, dievaluasi berdasarkan waktu eksekusi, throughput, dan penggunaan memori. Hasil penelitian menunjukkan bahwa RSA unggul dalam waktu eksekusi dan throughput, sedangkan Paillier lebih efisien dalam penggunaan memori dan mendukung komputasi aman langsung pada data terenkripsi. Skema hybrid RSA-Paillier yang diusulkan menawarkan kerangka kerja yang seimbang untuk keamanan data genomik, selaras dengan GDPR dan HIPAA, serta memastikan skalabilitas dalam aplikasi cloud berbasis dunia nyata.

Kata kunci: Enkripsi Homomorfik, RSA, Paillier, Kriptografi, Data Genomik, Cloud Computing