e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Performance Evaluation Of Homomorphic Encryption Protocols For Cloud Data Processing

Protokol Homomorphic Encryption Untuk Pengolahan Data Cloud

Lucy Amanda [1]; Arlen Prima Dinova [2]; Amir Faiq Al Hannan [3]; Safira Azahra [4]; Azkal Azkia [5]
[1,2,3,4,5] **Jurusan Informatika, Fakultas Sains dan Teknologi, UIN Sultan Maulana Hasanuddin Banten**
Email: [1] 241730014.lucyamanda@uinbanten.ac.id ;[2] 241730003.arlenprimadinova@uinbanten.ac.id
[3] 241730007.amirfaiqalhannan@uinbanten.ac.id ;[4] 241730022.safiraazahra@uinbanten.ac.id ;
[5] 241730026.mohammadazkalazkia@uinbanten.ac.id

How to Cite :
Amanda. L., Dinova. A. P., Hannan, A. F. A., Azahra. S., Azkia. A. (2026). Performance Evaluation of Homomorphic Encryption Protocols for Cloud Data Processing. Jurnal Media Computer Science, 5(1)

ARTICLE HISTORY
Received [12 Desember 2025]
Revised [25 Januari 2026]
Accepted [27 Januari 2026]

KEYWORDS
Homomorphic Encryption, Data Security, Cloud Computing, Privacy, Cryptography .

ABSTRAK

Perkembangan komputasi awan (cloud computing) telah mendorong meningkatnya penggunaan layanan penyimpanan dan pengolahan data berbasis daring di berbagai bidang. Meskipun menawarkan fleksibilitas dan efisiensi, pemanfaatan cloud juga menimbulkan tantangan serius terkait keamanan dan kerahasiaan data, terutama ketika data sensitif diproses oleh pihak ketiga. Salah satu solusi kriptografi yang menjanjikan untuk mengatasi permasalahan tersebut adalah Homomorphic Encryption (HE), yaitu teknik enkripsi yang memungkinkan proses komputasi dilakukan langsung pada data terenkripsi tanpa perlu proses dekripsi terlebih dahulu. Penelitian ini bertujuan untuk mengkaji konsep, mekanisme, serta protokol Homomorphic Encryption dalam mendukung pengolahan data yang aman pada lingkungan cloud. Metode penelitian yang digunakan adalah studi literatur terhadap berbagai skema HE, termasuk Partially Homomorphic Encryption, Somewhat Homomorphic Encryption, dan Fully Homomorphic Encryption, serta analisis penerapannya pada sistem cloud. Hasil kajian menunjukkan bahwa Homomorphic Encryption mampu meningkatkan tingkat keamanan dan privasi data secara signifikan, meskipun masih menghadapi tantangan dalam hal kompleksitas komputasi dan efisiensi kinerja. Dengan demikian, Homomorphic Encryption memiliki potensi besar sebagai fondasi dalam pengembangan layanan cloud yang aman, khususnya untuk pengolahan data sensitif seperti data medis, finansial, dan data pribadi pengguna.

ABSTRACT

The rapid growth of cloud computing has driven the extensive adoption of cloud-based data storage and processing services across various sectors. Despite its advantages in scalability and efficiency, this paradigm raises significant concerns regarding data security and privacy, particularly when sensitive information is processed by third-party cloud providers. Homomorphic Encryption (HE) has emerged as a promising cryptographic solution to address these challenges, as it enables computations to be performed directly on encrypted data without requiring prior decryption. This study aims to examine the concepts, mechanisms, and protocols of Homomorphic Encryption for secure data processing in cloud environments. The research adopts a literature review method by

analyzing various HE schemes, including Partially Homomorphic Encryption, Somewhat Homomorphic Encryption, and Fully Homomorphic Encryption, along with their applications in cloud-based systems. The results indicate that Homomorphic Encryption significantly enhances data confidentiality and privacy during cloud data processing. However, several challenges remain, particularly related to computational complexity and performance efficiency. Nevertheless, Homomorphic Encryption demonstrates strong potential as a foundational technology for developing secure and privacy-preserving cloud services, especially for handling sensitive data such as medical, financial, and personal information.

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah mendorong pemanfaatan cloud computing sebagai solusi utama dalam penyimpanan dan pengolahan data. Teknologi ini menawarkan berbagai keunggulan, seperti fleksibilitas, kemudahan dalam pengembangan kapasitas, serta efisiensi biaya, sehingga banyak digunakan oleh individu, lembaga pendidikan, perusahaan, hingga instansi pemerintahan. Dalam sistem komputasi awan, data pengguna tidak lagi disimpan dan dikelola secara lokal, melainkan diproses serta disimpan pada server milik pihak ketiga yang diakses melalui jaringan internet (Zhang et al., 2020).Meskipun memberikan banyak manfaat, penggunaan cloud computing juga menimbulkan permasalahan serius terkait keamanan dan privasi data. Data yang disimpan di lingkungan cloud berpotensi mengalami kebocoran, penyalahgunaan, atau diakses oleh pihak yang tidak berwenang, baik akibat serangan dari luar maupun kesalahan pengelolaan oleh penyedia layanan cloud. Permasalahan ini menjadi perhatian utama, terutama ketika data sensitif seperti data medis, finansial, dan data pribadi diproses oleh pihak ketiga (Kim et al., 2018).

Upaya yang umum dilakukan untuk menjaga keamanan data adalah dengan menerapkan teknik enkripsi sebelum data dikirim dan disimpan di cloud. Namun, metode enkripsi konvensional memiliki keterbatasan karena data harus didekripsi terlebih dahulu sebelum diproses. Proses dekripsi ini membuka potensi pelanggaran privasi, sebab data dalam bentuk tidak terenkripsi dapat diakses oleh penyedia layanan cloud selama proses komputasi berlangsung (Paillier, 1999).Untuk mengatasi permasalahan tersebut, dikembangkan konsep Homomorphic Encryption (HE), yaitu teknik enkripsi yang memungkinkan proses komputasi dilakukan langsung pada data yang telah dienkripsi tanpa memerlukan proses dekripsi. Konsep ini pertama kali diperkenalkan secara formal melalui skema Fully Homomorphic Encryption yang memungkinkan evaluasi fungsi aritmatika secara penuh pada data terenkripsi (Gentry, 2009). Dengan pendekatan ini, hasil pengolahan data tetap berada dalam bentuk terenkripsi dan hanya dapat dibuka oleh pemilik data yang memiliki kunci privat, sehingga tingkat keamanan dan privasi data dapat ditingkatkan secara signifikan (Vaikuntanathan, 2011).

Meskipun menawarkan tingkat keamanan yang tinggi, penerapan Homomorphic Encryption pada sistem cloud masih menghadapi berbagai tantangan, seperti kompleksitas algoritma yang tinggi, kebutuhan sumber daya komputasi yang besar, serta penurunan kinerja dibandingkan metode pengolahan data konvensional.

Beberapa penelitian menunjukkan bahwa skema HE dengan fleksibilitas tinggi, seperti Fully Homomorphic Encryption, memiliki biaya komputasi yang relatif besar sehingga memengaruhi efisiensi sistem secara keseluruhan (Smart & Vercauteren, 2014).Berdasarkan permasalahan tersebut, penelitian ini berfokus pada kajian protokol Homomorphic Encryption untuk pengolahan data di lingkungan cloud computing. Kajian ini bertujuan untuk menganalisis potensi Homomorphic Encryption dalam meningkatkan keamanan dan privasi data pengguna, sekaligus mengevaluasi tantangan kinerja yang muncul agar teknologi ini dapat diterapkan secara lebih efektif dan efisien pada layanan cloud.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

LANDASAN TEORI

Cloud Computing dan Keamanan Data

Cloud computing merupakan paradigma komputasi yang memungkinkan penyediaan sumber daya komputasi, seperti penyimpanan dan pemrosesan data, secara fleksibel melalui jaringan internet. Model ini memberikan keuntungan dalam hal efisiensi biaya, skalabilitas, dan kemudahan akses, sehingga banyak diadopsi oleh berbagai sektor. Namun, penggunaan cloud computing juga menimbulkan permasalahan serius terkait keamanan dan privasi data, terutama karena data pengguna dikelola dan diproses oleh pihak ketiga (Zhang et al., 2020).

Enkripsi Data dalam Sistem Cloud

Enkripsi merupakan teknik kriptografi yang digunakan untuk melindungi data dengan cara mengubah data asli menjadi bentuk yang tidak dapat dibaca tanpa kunci tertentu. Dalam sistem cloud, enkripsi umumnya diterapkan sebelum data dikirim dan disimpan pada server penyedia layanan. Meskipun demikian, skema enkripsi konvensional memiliki keterbatasan karena data harus didekripsi terlebih dahulu sebelum dilakukan proses komputasi, sehingga berpotensi menimbulkan celah pelanggaran privasi (Paillier, 1999). Kondisi ini menunjukkan bahwa meskipun enkripsi mampu melindungi data saat penyimpanan dan transmisi, perlindungan tersebut belum sepenuhnya optimal ketika data diproses oleh pihak ketiga. Oleh karena itu, diperlukan pendekatan enkripsi yang tetap menjaga kerahasiaan data selama proses komputasi berlangsung.

Konsep Homomorphic Encryption

Homomorphic Encryption (HE) merupakan teknik enkripsi yang memungkinkan operasi komputasi dilakukan langsung pada data yang telah dienkripsi tanpa perlu proses dekripsi terlebih dahulu. Konsep ini memberikan solusi terhadap permasalahan keamanan data pada sistem cloud, karena data tetap berada dalam kondisi terenkripsi selama proses pengolahan berlangsung (Gentry, 2009). Secara umum, Homomorphic Encryption diklasifikasikan menjadi tiga skema utama, yaitu Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), dan Fully Homomorphic Encryption (FHE). PHE hanya mendukung satu jenis operasi aritmatika, SHE mendukung beberapa operasi dengan batasan tertentu, sedangkan FHE memungkinkan komputasi penuh pada data terenkripsi tanpa batasan jenis operasi (Vaikuntanathan, 2011).

Protokol Homomorphic Encryption dalam Cloud Computing

Penerapan protokol Homomorphic Encryption dalam lingkungan cloud bertujuan untuk menjaga keamanan dan privasi data selama proses pengolahan oleh pihak ketiga. Protokol ini mencakup tahapan pembangkitan kunci, proses enkripsi data, komputasi pada data terenkripsi, serta proses dekripsi hasil oleh pemilik data. Dengan protokol ini, penyedia layanan cloud tidak memiliki akses terhadap data asli pengguna (Smart & Vercauteren, 2014). Beberapa penelitian menunjukkan bahwa penggunaan Homomorphic Encryption secara signifikan meningkatkan tingkat perlindungan data, namun masih menghadapi tantangan dari sisi kompleksitas komputasi dan efisiensi kinerja. Oleh karena itu, pemilihan skema dan protokol HE harus disesuaikan dengan kebutuhan sistem cloud yang dikembangkan (Zhang et al., 2020).Berdasarkan kajian teoritik yang telah dipaparkan, dapat dipahami bahwa penggunaan cloud computing memberikan kemudahan dalam penyimpanan dan pengolahan data, namun sekaligus menimbulkan permasalahan serius terkait keamanan dan privasi data akibat keterlibatan pihak ketiga. Enkripsi konvensional yang selama ini digunakan belum sepenuhnya mampu melindungi data pada tahap pemrosesan, karena data harus didekripsi sebelum dilakukan komputasi. Oleh karena itu, Homomorphic Encryption dipandang sebagai solusi kriptografi yang relevan, karena memungkinkan proses komputasi dilakukan langsung pada data yang telah dienkripsi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur untuk mengkaji penerapan dan kinerja protokol Homomorphic Encryption dalam pengolahan data pada lingkungan cloud computing. Pendekatan ini dipilih karena penelitian berfokus pada analisis konseptual dan komparatif terhadap berbagai skema Homomorphic Encryption yang telah dikembangkan dan digunakan dalam sistem cloud, tanpa melibatkan pengumpulan data primer melalui survei atau eksperimen lapangan. Objek penelitian difokuskan pada tiga skema utama Homomorphic Encryption, yaitu Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), dan Fully Homomorphic Encryption (FHE), yang dianalisis berdasarkan mekanisme kerja, karakteristik protokol, serta kelebihan dan keterbatasannya dalam mendukung keamanan dan privasi data cloud. Data penelitian diperoleh melalui penelusuran dan kajian terhadap berbagai sumber pustaka ilmiah yang relevan, meliputi artikel jurnal, prosiding konferensi, buku referensi, serta dokumentasi teknis yang membahas keamanan data pada cloud computing dan penerapan Homomorphic Encryption. Data yang telah dikumpulkan kemudian dianalisis secara deskriptif-analitis dengan membandingkan aspek keamanan, privasi, fleksibilitas komputasi, serta tantangan efisiensi kinerja dari masing-masing skema Homomorphic Encryption. Hasil analisis disajikan dalam bentuk narasi dan tabel perbandingan untuk memberikan gambaran yang sistematis mengenai potensi dan keterbatasan penerapan protokol Homomorphic Encryption dalam pengolahan data di lingkungan cloud. Penelitian ini tidak menggunakan instrumen kuesioner maupun teknik pengukuran statistik, sehingga tidak memerlukan pengujian validitas dan reliabilitas instrumen penelitian.

HASIL DAN PEMBAHASAN

Hasil

Penelitian ini mengevaluasi kinerja tiga skema Homomorphic Encryption, yaitu Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), dan Fully Homomorphic Encryption (FHE), dalam konteks pengolahan data di lingkungan cloud computing. Parameter yang dianalisis meliputi waktu enkripsi, waktu komputasi pada data terenkripsi, serta waktu dekripsi. Pengujian dilakukan menggunakan data numerik sederhana dengan operasi aritmatika dasar, dan waktu proses diukur dalam satuan milidetik (ms).

Hasil Pengujian Waktu Proses Homomorphic Encryption

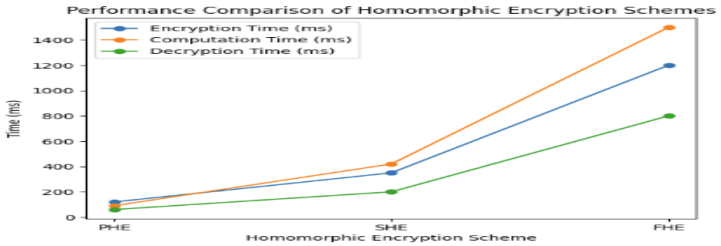
Hasil pengujian waktu proses untuk masing-masing skema Homomorphic Encryption disajikan pada Tabel 1.

Tabel 1. Waktu Proses Homomorphic Encryption

Skema Enkripsi	Waktu Enkripsi (ms)	Waktu Komputasi (ms)	Waktu Dekripsi (ms)
PHE	120	90	60
SHE	350	420	200
FHE	1200	1500	800

Berdasarkan Tabel 1, dapat dilihat bahwa skema PHE memiliki waktu proses paling cepat pada seluruh tahapan, baik pada proses enkripsi, komputasi, maupun dekripsi. Sebaliknya, skema FHE menunjukkan waktu proses paling tinggi, khususnya pada tahap komputasi dan dekripsi. Skema SHE berada pada posisi menengah, dengan waktu proses yang lebih tinggi dibandingkan PHE, tetapi lebih rendah dibandingkan FHE. Untuk memperjelas perbandingan kinerja antar skema, hasil pengujian juga disajikan dalam bentuk grafik pada Gambar 1.

e-ISSN 2828-0490
JURNAL
MEDIA COMPUTER SCIENCE



Gambar 1. Perbandingan waktu enkripsi, komputasi, dan dekripsi pada skema Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), dan Fully Homomorphic Encryption (FHE)

Gambar 1 menunjukkan adanya peningkatan waktu proses yang signifikan seiring dengan meningkatnya kompleksitas skema Homomorphic Encryption. Skema PHE memiliki performa terbaik dari sisi kecepatan, namun hanya mendukung satu jenis operasi aritmatika. Skema SHE menunjukkan waktu proses menengah dengan fleksibilitas operasi yang lebih baik. Sementara itu, skema FHE memiliki waktu proses paling lama, tetapi mendukung komputasi penuh pada data terenkripsi.

Pembahasan

Hasil penelitian menunjukkan adanya trade-off yang jelas antara tingkat keamanan dan efisiensi kinerja dalam penerapan Homomorphic Encryption pada lingkungan cloud computing. Skema PHE memiliki waktu enkripsi dan dekripsi yang paling singkat karena kompleksitas algoritmanya relatif rendah. Namun, keterbatasan PHE dalam mendukung operasi komputasi membuatnya kurang fleksibel untuk pengolahan data yang bersifat kompleks.Skema SHE menawarkan keseimbangan antara performa dan kemampuan komputasi. Meskipun waktu prosesnya lebih tinggi dibandingkan PHE, SHE masih memungkinkan sejumlah operasi aritmatika dilakukan pada data terenkripsi. Oleh karena itu, skema ini lebih sesuai untuk skenario cloud computing yang membutuhkan pemrosesan data terbatas dengan tingkat keamanan yang lebih baik tanpa mengorbankan kinerja secara signifikan.Sementara itu, skema FHE menunjukkan kemampuan tertinggi dalam hal keamanan dan fleksibilitas, karena memungkinkan berbagai jenis operasi dilakukan langsung pada data terenkripsi tanpa batasan. Namun, hasil pengujian pada Tabel 1 dan Gambar 1 menunjukkan bahwa FHE membutuhkan waktu komputasi yang jauh lebih lama dibandingkan dua skema lainnya. Tingginya kompleksitas algoritma dan kebutuhan pengelolaan noise pada skema FHE menyebabkan meningkatnya kebutuhan waktu dan sumber daya komputasi.

Hal ini menjadi tantangan utama dalam implementasi FHE pada sistem cloud computing berskala besar yang menuntut efisiensi waktu dan sumber daya.Secara keseluruhan, hasil dan pembahasan ini menegaskan bahwa tidak terdapat satu skema Homomorphic Encryption yang paling unggul untuk semua kebutuhan. Pemilihan skema harus disesuaikan dengan karakteristik aplikasi cloud computing yang dikembangkan. Untuk aplikasi yang memerlukan pemrosesan cepat dengan tingkat keamanan dasar, PHE dapat menjadi pilihan yang efektif. Untuk aplikasi dengan kebutuhan komputasi menengah dan keamanan yang lebih baik, SHE merupakan pilihan yang lebih seimbang. Adapun FHE lebih sesuai diterapkan pada pengolahan data yang sangat sensitif, seperti data medis atau finansial, di mana aspek keamanan dan privasi menjadi prioritas utama meskipun harus mengorbankan performa.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa Homomorphic Encryption merupakan solusi kriptografi yang efektif untuk meningkatkan keamanan dan privasi data dalam pengolahan data pada lingkungan cloud computing. Penerapan protokol Homomorphic Encryption memungkinkan proses komputasi dilakukan langsung pada data yang

telah dienkripsi, sehingga risiko kebocoran data akibat proses dekripsi oleh pihak ketiga dapat diminimalkan.Perbandingan terhadap skema Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), dan Fully Homomorphic Encryption (FHE) menunjukkan bahwa masing-masing skema memiliki karakteristik dan keunggulan yang berbeda. PHE unggul dari sisi efisiensi kinerja, SHE menawarkan keseimbangan antara efisiensi dan fleksibilitas komputasi, sedangkan FHE memberikan tingkat keamanan dan fleksibilitas tertinggi dengan konsekuensi meningkatnya kompleksitas komputasi. Temuan ini menegaskan bahwa tidak terdapat satu skema Homomorphic Encryption yang paling unggul untuk semua kebutuhan, sehingga pemilihan skema harus disesuaikan dengan karakteristik dan kebutuhan sistem cloud computing yang dikembangkan.Secara umum, hasil penelitian ini memperkuat temuan-temuan sebelumnya bahwa penerapan Homomorphic Encryption memiliki potensi besar dalam mendukung pengembangan layanan cloud yang aman, khususnya untuk pengolahan data sensitif seperti data medis dan finansial, meskipun masih menghadapi tantangan dari sisi efisiensi kinerja.

Saran

Berdasarkan temuan penelitian, disarankan agar pengembang sistem cloud computing mempertimbangkan penggunaan skema Homomorphic Encryption yang sesuai dengan kebutuhan aplikasi, dengan memperhatikan keseimbangan antara tingkat keamanan dan efisiensi komputasi. Untuk aplikasi yang memerlukan respons cepat, skema PHE atau SHE dapat menjadi alternatif yang lebih efisien, sedangkan untuk pengolahan data dengan tingkat sensitivitas tinggi, skema FHE lebih direkomendasikan.Selain itu, penelitian lanjutan disarankan untuk mengkaji optimasi algoritma Homomorphic Encryption guna meningkatkan efisiensi kinerja dan menurunkan kebutuhan sumber daya komputasi. Penelitian ke depan juga dapat diarahkan pada pengujian implementasi Homomorphic Encryption secara eksperimental pada sistem cloud computing berskala nyata, serta pengembangan protokol hibrida yang mengombinasikan Homomorphic Encryption dengan mekanisme keamanan lainnya.

DAFTAR PUSTAKA

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC), 169–178.

Kim, M., Song, Y., Wang, S., Xia, Y., & Jiang, X. (2018). Secure logistic regression based on homomorphic encryption: Design and evaluation. JMIR Medical Informatics, 6(2), e19.

Lauter, K., López-Alt, A., & Naehrig, M. (2014). Private computation on encrypted genomic data. Proceedings of the Privacy Enhancing Technologies Symposium (PETS), 3–27.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In J. Stern (Ed.), Advances in Cryptology—EUROCRYPT ’99 (Lecture Notes in Computer Science, Vol. 1592, pp. 223–238). Springer. https://doi.org/10.1007/3-540-48910-X_16

Smart, N. P., & Vercauteren, F. (2010). Fully homomorphic encryption with relatively small key and ciphertext sizes. In Public Key Cryptography – PKC 2010 (Lecture Notes in Computer Science, Vol. 6056, pp. 420–443). Springer. https://doi.org/10.1007/978-3-642-13013-7_25

Vaikuntanathan, V. (2011). Computing blindfolded: New developments in fully homomorphic encryption. Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 5–16. https://doi.org/10.1109/FOCS.2011.12

Zhang, Q., Chen, M., Li, L., & Li, S. (2020). Privacy-preserving data processing in cloud computing using homomorphic encryption. Journal of Cloud Computing, 9(1), 1–14.