JNATIA Volume 3, Nomor 2, Februari 2025 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Pengamanan Data Finansial Menggunakan Enkripsi Homomorfik Pailler

Ida Bagus Made Wiguna Tedja Sukmana[a1], Agus Muliantara[a2]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]gustedja123@gmail.com
[2]muliantara@unud.ac.id

Abstract

In the current digital era, concerns about data privacy are increasing due to the ease of data creation, storage, access, and dissemination. To protect sensitive data, such as financial information and identities, effective methods are needed to safeguard privacy from unauthorized access. One such method is homomorphic encryption, which allows computations to be performed on encrypted data without the need for decryption. This research implements the Paillier Cryptosystem in financial data security, specifically for customer savings accounts. The encryption and computation processes on savings data are performed using homomorphic encryption, ensuring data confidentiality and customer privacy. The testing results demonstrate that the system can perform homomorphic computations effectively, producing results consistent with plaintext calculations. In conclusion, the use of homomorphic encryption in financial data security can enhance privacy, security, and data reliability while providing more control to data owners.

Keywords: *Cryptography, Encryption, Homomorphic Encryption, Data Security, Paillier Cryptosystem*

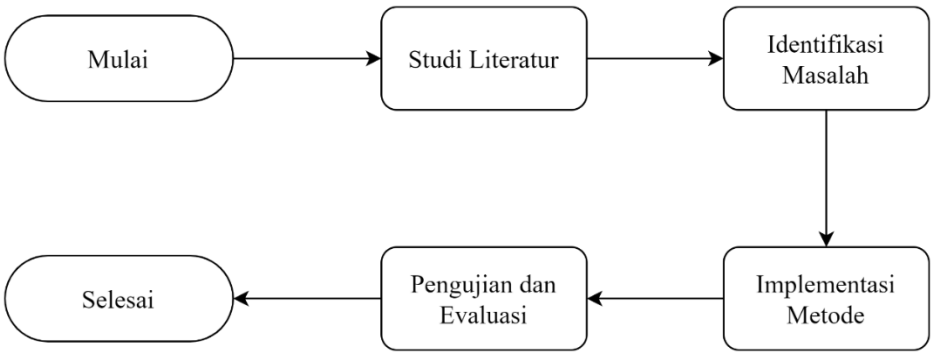
1. Pendahuluan

Di era digital ini, data-data dengan sangat mudah dibuat, disimpan, diakses, dan disebarkan. Dengan kemudahan tersebut, kekhawatiran akan privasi data kita semakin meningkat. Privasi diperlukan di berbagai jenis data, contohnya informasi keuangan, identitas, dan alamat. Jika terjadi kebocoran data yang meliputi informasi finansial, korban dapat mengalami kerugian harta termasuk pembobolan akun rekening. Maka dari itu diperlukan metode untuk menjaga privasi data tersebut dari pihak tidak berwenang. Terdapat beragam metodologi untuk menjaga privasi data[1] seperti Anonimisasi yang melibatkan penghapusan atau perubahan komponen-komponen yang dapat diidentifikasi dalam *dataset*, sehingga melindungi identitas individu sambil memungkinkan analisis dan penggunaan yang sah; Privasi diferensial yang memperkenalkan kebisingan atau ketidakpastian ke dalam respons kueri, menjaga privasi kontribusi individu dalam *dataset* sambil mempertahankan akurasi statistik; Enkripsi yang mengamankan data dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Metodologi ini memastikan kerahasiaan, bahkan dalam kasus akses yang tidak sah. Enkripsi mengubah informasi yang dapat dipahami manusia atau yang disebut *plaintext* dengan algoritma tertentu menjadi bentuk yang tidak dapat dipahami atau yang disebut *ciphertext*. Enkripsi biasanya dilakukan untuk kepentingan militer, namun dengan perkembangan teknologi informasi enkripsi juga dilakukan kepada transmisi data melalui internet untuk menjaga privasi data pengguna. Enkripsi dapat dilakukan dengan banyak cara, salah satunya adalah enkripsi homomorfik. Enkripsi homomorfik memiliki cara unik untuk melindungi data. Enkripsi homomorfik memungkinkan data untuk dihitung saat dalam keadaan terenkripsi, tanpa perlu didekripsi terlebih dahulu. Dengan kata lain, data dapat dilakukan operasi matematika dan komputasi dalam bentuk *ciphertext* tanpa harus mengembalikannya ke bentuk *plaintext*. Hal ini sangat berguna karena memungkinkan analisis dan pengolahan data yang aman, tanpa mengorbankan keamanan privasi.

Kajian sebelumnya telah mengimplementasikan enkripsi homomorfik ke dalam sistem *electronic voting* menggunakan skema *Paillier Cryptosystem* dalam jumlah vote kandidat dan dalam penjumlahan vote setiap kandidat[2]. Di sistem tersebut, pemilih perlu melakukan login terlebih dahulu melalui *face-recognition* untuk mendapatkan akses melakukan pemilihan suara. Suara dari pemilih kemudian dienkripsi dengan *paillier* yang kemudian dimasukkan ke *database mysql*. Kandidat yang dipilih, *ciphertext* mereka akan ditambah nilai satu sehingga *ciphertext* berubah. Penelitian ini akan mengimplementasikan P*aillier Cryptosystem* untuk keamanan data finansial seperti tabungan. Paillier cryptosystem dipilih dalam penelitian ini karena merupakan jenis enkripsi homomorfik yang memungkinkan operasi penambahan dan pengurangan dilakukan langsung pada data yang terenkripsi tanpa perlu melakukan dekripsi terlebih dahulu. Hal ini memungkinkan proses komputasi dilakukan tanpa mengungkapkan informasi sensitif dalam bentuk plaintext, yang sangat penting untuk menjaga privasi data finansial nasabah. Selain itu, Paillier Cryptosystem juga menawarkan tingkat keamanan yang tinggi, terutama dalam konteks keamanan kriptografi modern. Kombinasi dari kemampuan homomorfik dan keamanan yang tinggi membuat Paillier Cryptosystem menjadi pilihan yang tepat untuk aplikasi keamanan data finansial seperti tabungan. Oleh karena itu, penelitian ini memilih enkripsi homomorfik Paillier Cryptosystem sebagai solusi untuk menjaga privasi finansial nasabah dari pihak yang tidak berwenang. Dalam implementasinya di sistem, hal pertama yang akan dilakukan adalah generasi kunci privat dan publik untuk setiap nasabah. Setelah itu, tabungan nasabah dapat dilakukan penambahan atau pengurangan saldo dalam bentuk *ciphertext* dengan jumlah saldo yang terenkripsi. Hal ini membantu menjaga privasi finansial nasabah dari pihak yang tidak berwenang.

2. Metode Penelitian

Penelitian akan dilakukan sesuai dengan flowchart pada gambar 1.



Gambar 1. *Flowchart* Penelitian

2.1. Identifikasi Masalah

Pada tahap ini, peneliti memahami permasalahan yang ingin dipecahkan. Permasalahan yang dibawakan dalam penelitian ini adalah rentannya informasi finansial nasabah, seperti saldo tabungan dan transaksi, sangat sensitif dan rentan terhadap serangan siber. Tanpa enkripsi yang tepat, data ini dapat diretas atau dicuri, mengakibatkan kerugian finansial dan pencurian identitas bagi nasabah. Selain itu, nasabah memiliki hak untuk menjaga privasi informasi keuangan mereka. Namun, dalam sistem konvensional, pihak bank atau pihak lain yang terlibat dalam pemrosesan transaksi dapat mengakses data tabungan nasabah. Maka dari itu, enkripsi homomorfik memungkinkan pemrosesan data yang aman tanpa mengorbankan privasi nasabah.

2.2. Enkripsi Homomofik

Enkripsi homomorfik adalah metode enkripsi yang memungkinkan terjadinya proses komputasi antara *ciphertext* layaknya *plaintext* tanpa perlu di-dekripsi terlebih dahulu. Melakukan komputasi pada data yang terenkripsi berarti bahwa jika seorang pengguna memiliki fungsi f dan ingin

mendapatkan f(m1, . . . , mn) untuk beberapa input m1, . . . , mn, maka dimungkinkan untuk melakukan komputasi pada enkripsi dari input ini, c1, . . . , cn, dan mendapatkan hasil yang didekripsi menjadi f(m1, . . . , mn) [3]. Nilai fitur ini sangat bermanfaat dan berharga untuk privasi data. Ketika kita mengenkripsi data kita, bahkan jika penyedia layanan atau pengolah data lainnya dapat mengaksesnya, mereka tidak dapat memahami isinya. Ini berarti risiko kebocoran data pribadi yang sensitif secara signifikan berkurang, sambil juga memberikan lebih banyak kontrol kepada pemilik data [4].

2.3. *Paillier Cryptosystem*

Paillier cryptosystem adalah enkripsi homomorfik aditif yang diajukan oleh Paillier pada tahun 1999[5]. Sistem ini memiliki kunci publik untuk melakukan enkripsi dan kunci privat untuk melakukan dekripsi. Enkripsi homomorfik aditif berarti *ciphertext* dari enkripsi ini dapat melakukan operasi penambahan pada data yang terenkripsi lainnya dan kemudian mendapatkan hasilnya dalam teks biasa setelah dekripsi.

Adapun langkah-langkah generasi kunci sebagai berikut:

a. Pilih dua bilangan prima besar p dan q secara acak dan independen. Pastikan bahwa

$$\gcd\big(pq,(p-1)(q-1)\big)=1 \quad (1)$$

gcd adalah *greatest common divisor* atau faktor persekutuan terbesar. Jika gcd tidak sama dengan 1, ulangi lagi.

b. Hitung nilai

$$n=pq \quad (2)$$

dan

$$\lambda=lcm(p-1,q-1) \quad (3)$$

lcm adalah least common multiple atau Kelipatan persekutuan terkecil

c. Pilih sebuah bilangan bulat acak g dimana g adalah bilangan bulat antara 1 dan n2

$$g \in \mathbb{Z}^*_{n^2} \quad (4)$$

d. Hitung invers modular dari

$$\mu=(L\big(g^{\lambda} mod\ n^2\big))^{-1} mod\ n \quad (5)$$

Dimana fungsi L didefinisikan dengan

$$L(u)=\frac{u-1}{n} \quad (6)$$

multiplicative inverse hanya ada jika dan hanya jika nilai generator valid telah didapat dari tahap sebelumnya.

e. Kunci publik adalah pasangan (n,g). Kunci ini digunakan untuk proses enkripsi.

f. Kunci privat adalah (λ,μ). Kunci ini digunakan untuk proses dekripsi.

Enkripsi pesan m dapat dilakukan dengan cara berikut:

a. $m \in \mathbb{Z}_n$ (7)

Jadi enkripsi dapat bekerja selama $0 \leq m < n$

b. Pilih nilai acak r dalam range $0 < r < n$

c. Hitung *ciphertext* dengan persamaan:

$$c = g^m . r^n \ mod \ n^2 \quad (8)$$

Dekripsi pesan c dapat dilakukan dengan cara berikut:

a. $c \in \mathbb{Z}_{n^2}$ (9)

Jadi enkripsi dapat bekerja selama $0 \leq c < n^2$

b. Hitung *plaintext* dengan persamaan:

$$m = L\left(c^{\lambda} mod \ n^2\right).\mu \ mod \ n \quad (10)$$

Adapun properti homomorfik dari paillier cryptosystem sebagai berikut:

a. Produk perkalian dari dua buah *ciphertext* akan ter-dekripsi menjadi hasil penjumlahan *plaintext* terkait.

$$D(E(m_1, r_1).E(m_2, r_2) \ mod \ n^2) = m_1 + m_2 \ mod \ n \quad (11)$$

b. Produk dari perkalian *ciphertext* dengan plaintext yang ditingkatkan ke g akan ter-dekripsi menjadi jumlah dari teks terkait.

$$D(E(m_1, r_1).g^{m_2} \ n^2) = m_1 + m_2 \ mod \ n \quad (12)$$

2.4. Rancangan Pengujian

Pengujian yang akan dilakukan adalah pengamanan data saldo nasabah dan penambahan serta pengurangan saldo tersebut dalam bentuk *ciphertext*. Pengujian ini dilakukan untuk mengetahui apakah sistem dapat melakukan melakukan komputasi homomorfik. Waktu eksekusi juga dihitung saat melakukan komputasi dan key generation dengan perulangan sebanyak 50 kali. Pengujian kali ini tidak serta mengujikan aplikasi dikarenakan aplikasi untuk sistem ini masih dalam tahap perancangan.

3. Hasil dan Diskusi

3.1. Pengujian Sistem

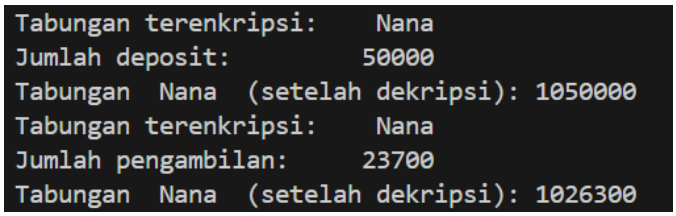
a. Enkripsi

```
Masukkan nama: Nana
Masukkan saldo awal: 1000000
Ciphertext: 55958745525720564779552367889191845825985144704618128104916151224315115977468133997688753318718431306389043123249635193902249021033107783904678897276951285948682839160554992518271989158736701392299037612094213958420946401986150143915968439709701398129308453025204507589644978999501749232991731851745124464596748742409245772510148305891886458788664395822269247415760185663816298596528406282638297414415620596036558231791359688376288746117757251235216218396503550514165904688079553511586494363456889624529541754936472283176888980821984429933676781191111196039286804608901582213997742668003728764232846089233114096427961200590890740954984940016235768076329751646286133253138414355555178319260950577004372190888119722367315296869436076646240547009448742793583484321316763483753356486191148172889666761221920967732190510987771077010940452019271638362743780063882366941203576909665090437909111183376600891651786698291717973902213947067505691327963728540401352491668858659708681679270972006632200370287793233112484277224246873569873388735316295316439914434844119158621683293686772389688478523130592754928073930865172065667991239121568736920297920553993117375157529845252902657238002502092140498619480549504098496620047421749640006911780434756229943166494836948365236068616493015434001740073065955236893992228604375712327382118980187929523390596326857281906297875494446282915060824631036348516895542486145335182539619171566060045643302336096893422289202131497847740935164570207720288147886015070656499942940850786693251435587597774163148726958703490348391143218271135987045156540802312045872496967142220372887483593176436785250222735291086745950210396723093471591666984580586310230581404815873051260101627819700408580557116875466689242785547966964794940404730132806822604004560285274350110248368301890089862527347246274193960287730075401938369132646200585 27
```

Gambar 2. *Output* Enkripsi

Proses dimulai dengan pembuatan objek nasabah1 dan diberikan nama dan saldo awal. Saldo awal tersebut akan diubah menjadi *ciphertext* sebelum disimpan. Pada gambar 2, saldo awal yang dimasukkan adalah 1.000.000 yang kemudian dijadikan *ciphertext*. Rata-rata waktu eksekusi yang diperlukan untuk membuat objek nasabah tersebut dalam 50 kali percobaan adalah sebanyak 4,270 detik.

b. Komputasi



Gambar 3. *Output* Komputasi

Penambahan dan pengurangan dilakukan kepada tabungan nasabah1. Jumlah deposit saldo dan penarikan diubah menjadi *ciphertext* sebelum dihitung bersama dengan tabungan yang sudah ada di objek. Hasil komputasi yang telah didekripsi sesuai dengan jumlah perhitungan *plaintext*. Setelah dilakukan percobaan sebanyak 50 kali, didapatkan total waktu waktu 7,230 detik, sehingga rata-rata waktu yang diperlukan adalah 0.347 detik

c. Keamanan
Dari segi keamanan, sistem kriptografi Paillier adalah sebuah sistem kriptografi kunci publik dengan keamanan semantik. Untuk menghitung dan menilai kelebihan redundansi n kali pada $\mathbb{Z}_{n^2}^*$ dalam kriptosistem paillier sangat sulit, sehingga kriptosistem Paillier memiliki tingkat keamanan yang tinggi. Selain itu, dalam proses enkripsi, karena sifat acak dari nilai r, bahkan jika plaintext yang sama dienkripsi setiap kali, akan dihasilkan ciphertext yang berbeda. Oleh karena itu, sulit untuk melakukan serangan dengan menggunakan plaintext, dan keamanan algoritma tersebut meningkat secara proporsional[6]. Sebagai contoh, jika kita menggunakan kunci 2048-bit, itu berarti modulus n dalam algoritma Paillier memiliki panjang 2048-bit. Kunci 2048-bit dianggap setara dengan kekuatan keamanan 112-bit, itu berarti akan membutuhkan sekitar 2^{112} operasi dasar untuk memecahkan kunci dengan serangan brute force.

4. Kesimpulan

Berdasarkan hasil percobaan, enkripsi saldo dapat dilakukan yang kemudian disimpan sehingga jumlah saldo nasabah tidak dapat dipahami jumlahnya. Hal ini membantu melindungi privasi dan keamanan data dari akses yang tidak sah. Dengan menggunakan teknik enkripsi, bahkan jika data tersebut diakses oleh pihak yang tidak berwenang, mereka tidak akan dapat membaca atau memanipulasi informasi tersebut. Proses komputasi juga dilakukan pada data yang terenkripsi, yang kemudian didekripsi untuk menghasilkan hasil yang sesuai dengan perhitungan aslinya. Untuk penelitian yang akan datang terdapat hal yang harus dikembangkan, yaitu penyimpanan data pada sebuah database seperti mysql.

Daftar Pustaka

[1] P. Mwiinga, “Privacy-Preserving Technologies: Balancing Security and User Privacy in the Digital Age”, Dec. 2023, doi: 10.5281/zenodo.10406538.
[2] A. Rajak and R. Agustia, "Purwarupa Sistem E-Voting Menggunakan Enkripsi Homomorphic Di Komisi Pemilihan Umum Kota Bandung," Jurnal Penelitian Mahasiswa Teknik Dan Ilmu Komputer (JUPITER), vol. 1, pp. 1–10, 2021, doi: 10.34010/jupiter.v1i1.5403.
[3] F. Armknecht, C. Boyd, C. Carr, K. Gjøsteen, A. Jäschke, C. A. Reuter, and M. Strand, "A Guide to Fully Homomorphic Encryption," IACR ePrint Archive, 2015. [Online]. Available:

https://eprint.iacr.org/2015/1192.
[4] B. Li, D. Li, and M. Zhu, "Application analysis of data encryption technology," Applied and Computational Engineering, vol. 50, pp. 199–205, 2024, doi: 10.54254/2755-2721/50/20241502.
[5] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1999, doi: 10.1007/3-540- 48910-X_16.
[6] E, M., & Geng, Y. Homomorphic Encryption Technology for Cloud Computing. *Procedia Computer Science*, *154*, 73–83, 2019. https://doi.org/10.1016/j.procs.2019.06.012