PENGAMANAN DATABASE MENGGUNAKAN MODEL HIBRID BLOCKCHAIN DAN HOMOMORPIC ENCRYPTION DENGAN OPTIMASI ZERO-KNOWLEDGE PROOF

Deden Pratyaten[1], Muhammad Muzammil[2], Nadia Cahaya Islami[3], Kartika Imam Santoso[4], Eko Supriyadi[5]
Universitas An Nuur

Email: dprastyaten@gmail.com[1], muzammilselojari@gmail.com[2], nadiachy292@gmail.com[3], kartikaimams@gmail.com[4], ekalaya56@gmail.com[5]

ABSTRACT

Database security has become a crucial issue with the increasing cyber threats and data breaches that significantly impact organizations and individuals. This research proposes an innovative hybrid model that integrates blockchain technology, homomorphic encryption, and zero-knowledge proof to secure databases. This approach offers a multi-layer security mechanism that enables user identity verification without exposing credentials, encrypted data processing, and immutable access tracking. The research method uses an experimental approach with attack simulations on databases implemented with and without the proposed hybrid model. Results show significant improvements in resistance against SQL injection attacks (99.7%), man-in-the-middle attacks (98.2%), and unauthorized access (100%) compared to conventional methods. Although there is a trade-off in the form of a 12% latency increase, this hybrid model offers an optimal balance between security and performance. The main contribution of this research is the development of zero-knowledge proof integration algorithm that optimizes the verification process by reducing computational overhead by 35% compared to conventional implementations.

Keywords: *blockchain; databasesecurity; ecryption; homomorphic; proof security hybridization; zero-knowledge*

Correspondence:
Penulis : Muhammad Muzammil
Email; muzammilselojari@gmail.com

PENDAHULUAN

Keamanan database merupakan komponen fundamental dalam arsitektur sistem informasi modern yang menghadapi tantangan keamanan semakin kompleks. Menurut laporan IBM Security (2023), biaya rata-rata kebocoran data global mencapai USD 4,45 juta pada tahun 2023, meningkat 15% dalam lima tahun terakhir. Di Indonesia, BSSN mencatat 1.872 insiden serangan siber pada triwulan pertama 2023, dengan 38,2% menargetkan database organisasi (BSSN, 2023). Statistik ini menggarisbawahi urgensi pengembangan mekanisme keamanan

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

database yang lebih komprehensif dan tangguh.

Metode keamanan konvensional seperti *enkripsi*, *access control list* (ACL), dan *audit logging* telah banyak diimplemen-tasikan, namun memiliki keterbatasan fundamental yang dapat dieksploitasi oleh aktor jahat. *Enkripsi* konvensional mengharuskan data didekripsi untuk diproses, menciptakan kerentanan selama pemrosesan (Sharma & Chen, 2023). ACL rentan terhadap *privilege escalation* dan *credential theft* (Liu et al., 2023). Sistem *audit logging* konvensional dapat dimanipulasi oleh penyerang dengan akses administratif (Rahman et al., 2023).

Blockchain menawarkan struktur data terdesentralisasi dengan sifat *immutability* yang meningkatkan integritas dan transparansi akses database (Crosby et al., 2016). *Homomorphic encryption* memung-kinkan komputasi pada data terenkripsi tanpa dekripsi (Gentry, 2009). *Zero-knowledge proof* memungkinkan verifikasi tanpa mengungkapkan informasi sensitif (Goldwasser et al., 2019). Namun, implementasi individu teknologi ini menghadapi tantangan seperti *overhead* performa dan kompleksitas implementasi.

Penelitian ini bertujuan mengem-bangkan dan mengevaluasi model hibrid yang mengintegrasikan *blockchain*, *homomor-phic encryption encryption*, dan *zero-knowledge proof* untuk menciptakan sistem keamanan database yang tangguh dan adaptif.

A. Rumusan Masalah**:**

1. Bagaimana mengembangkan model hibrid yang mengintegrasikan *blockchain*, *homomorphic encryption*, dan *zero-knowledge proof* untuk keamanan database?
2. Seberapa efektif model hibrid ini dalam menghadapi berbagai serangan terhadap database?
3. Bagaimana performa model hibrid dibandingkan dengan metode keamanan database konvensional?

B. Tujuan Penelitian:

1. Mengembangkan model hibrid inovatif untuk keamanan database.
2. Mengevaluasi efektivitas model hibrid terhadap serangan database.
3. Menganalisis performa model hibrid dibandingkan metode konvensional.

C. Manfaat Penelitian:

1. Memberikan kontribusi teoretis berupa model hibrid keamanan database.
2. Menyediakan solusi praktis untuk meningkatkan keamanan database organisasi, meningkatkan keamanan database organisasi.
3. Menjadi referensi untuk penelitian lanjutan dalam keamanan database.

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

METODE PENELITIAN

A. Rancangan Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan desain komparatif untuk mengembangkan dan mengevaluasi model hibrid keamanan database. Pendekatan ini memungkinkan pengembangan model secara iteratif dan evaluasi komprehensif terhadap efektivitas keamanan dan performa.

B. Pengembangan Model Hibrid

Model hibrid yang diusulkan mengintegrasikan tiga komponen utama: blockchain, homomorphic encryption, dan zero-knowledge proof. Integrasi ini dilakukan dengan arsitektur modular yang memungkinkan masing-masing komponen beroperasi secara independen namun saling terhubung melalui interface standar.

1. Komponen Blockchain

Komponen blockchain berfungsi sebagai immutable ledger untuk mencatat semua aktivitas akses dan modifikasi database. Implementasi menggunakan private blockchain dengan konsensus Practical Byzantine Fault Tolerance (PBFT) yang dioptimalkan untuk lingkungan database. Setiap transaksi akses database direpresentasikan sebagai blok yang berisi informasi berikut:

a. Hash dari identitas pengguna yang diverifikasi melalui zero-knowledge proof
b. Timestamp transaksi
c. Jenis operasi database (SELECT, INSERT, UPDATE, DELETE)
d. Hash dari query yang dieksekusi
e. Hash dari data yang diakses/dimodifikasi

Algoritma konsensus PBFT yang dimodifikasi digunakan untuk memvalidasi blok dengan kompleksitas waktu $O(n^2)$, di mana n adalah jumlah node validator. Modifikasi dilakukan untuk mengoptimalkan performa dalam konteks operasi database dengan formulasi sebagai berikut:

Algorithm 1: Modified PBFT Consensus for Database Transactions

Input: Transaction T, Validator set $V = \{v_1, v_2, ..., v_n\}$

Output: Validated block B

a. Primary validator v_p creates pre-prepare message M_pp = (v, n, d, T)
b. where v is view number, n is sequence number, d is digest of T
c. Broadcast M_pp to all validators in V
d. Each validator v_i verifies:
   - Signature of M_pp is valid
   - Transaction T conforms to database access policy
   - v_i has not accepted another pre-prepare message with same v and n

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

e. If verification passes, v_i sends prepare message M_p = (v, n, d, i) to all validators
f. Each validator collects prepare messages until it has 2f+1 valid messages
g. (where f is maximum number of faulty validators allowed)
h. When validator has 2f+1 prepare messages, it enters prepared state and
i. sends commit message M_c = (v, n, i) to all validators
j. Each validator collects commit messages until it has 2f+1 valid messages
k. When validator has 2f+1 commit messages, transaction T is committed as block B
l. Block B is added to blockchain

C. Komponen Homomorphic Encryption

Komponen homomorphic encryption memungkinkan operasi query dilakukan pada data terenkripsi tanpa perlu mendekripsinya. Penelitian ini mengimplementasikan skema Somewhat Homomorphic Encryption (SHE) yang mengoptimalkan performa dengan memungkinkan jumlah operasi terbatas pada ciphertext. SHE dipilih karena overhead komputasi yang lebih rendah dibandingkan Fully Homomorphic Encryption (FHE), dengan tetap mendukung operasi database yang umum.

Proses enkripsi dan operasi homomorphic didefinisikan sebagai berikut:

a. Enkripsi: $Enc(pk, m) \rightarrow c$, di mana pk adalah public key, m adalah plaintext, dan c adalah ciphertext
b. Dekripsi: $Dec(sk, c) \rightarrow m$, di mana sk adalah secret key
c. Operasi aditif: $Enc(pk, m_1) \oplus Enc(pk, m_2) = Enc(pk, m_1 + m_2)$
d. Operasi multiplikatif: $Enc(pk, m_1) \otimes Enc(pk, m_2) = Enc(pk, m_1 \times m_2)$

Untuk mengoptimalkan performa, implementasi SHE menggunakan Ring-Learning With Errors (Ring-LWE) dengan parameter sebagai berikut:

a. Derajat polinomial n = 4096
b. Modulus $q = 2^{32}$
c. Error distribution χ = discrete Gaussian dengan standar deviasi $\sigma = 3.2$

Skema ini memungkinkan hingga 10 operasi multiplikatif berturut-turut sebelum noise dalam ciphertext mencapai ambang batas yang memerlukan refresh ciphertext. Operasi refresh menggunakan teknik bootstrapping yang dioptimalkan dengan kompleksitas O(n log n) melalui implementasi Fast Fourier Transform (FFT).

D. Komponen Zero-Knowledge Proof

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

Komponen zero-knowledge proof (ZKP) berfungsi untuk verifikasi identitas dan otorisasi tanpa mengungkapkan kredensial sensitif.

Penelitian ini mengimplementasikan protokol zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) yang dioptimalkan untuk aplikasi database.

Protokol ZK-SNARK yang diimplementasikan menggunakan kurva eliptik BLS12-381 dengan kompleksitas verifikasi O(1). Kontribusi utama dalam penelitian ini adalah optimasi algoritma ZKP untuk mengurangi overhead komputasi verifikasi sebesar 35% melalui teknik batching dan paralelisasi yang dirumuskan sebagai berikut:

Algorithm 2: Optimized ZK-Proof Verification for Database Access

Input: Public input x, Proof $\pi = (\pi_a, \pi_\beta, \pi_k)$, Verification key vk

Output: Boolean (accept/reject)

a. Batch multiple verification requests into vector $V = \{(x_1, \pi_1), (x_2, \pi_2), ..., (x_n, \pi_n)\}$
b. Compute common pairing products $P\_common = e(vk.\alpha, vk.\beta)$
c. For each (x_i, π_i) in V in parallel:
   - Compute input-specific terms:
     $T_1 = e(\pi_i.a, \pi_i.b)$
     $T_2 = e(vk.\gamma, \pi_i.k)$
     $T_3 = e(x_i \cdot vk.\gamma, vk.\beta)$
   - Verify $T_1 \cdot T_2 = P\_common \cdot T_3$
4. Aggregate results and return acceptance if all verifications pass

E. **Komponen Zero-Knowledge Proof**

Integrasi ketiga komponen dilakukan melalui layer middleware yang mengoordinasikan interaksi antar komponen. Alur kerja sistem secara keseluruhan dapat dijelaskan sebagai berikut:

1. Pengguna mengirimkan request akses database bersama dengan bukti ZKP untuk verifikasi identitas dan otorisasi.
2. Komponen ZKP memverifikasi bukti tanpa mengungkap kredensial pengguna.
3. Jika verifikasi berhasil, request diproses melalui komponen homomorphic encryption, yang memungkinkan operasi database pada data terenkripsi.
4. Semua aktivitas akses dan modifikasi dicatat dalam blockchain sebagai transaksi yang divalidasi melalui konsensus PBFT yang dimodifikasi.
5. Hasil query dikembalikan ke pengguna dalam bentuk terenkripsi, yang dapat didekripsi hanya oleh pengguna dengan kunci yang valid.

Kompleksitas integrasi ini dikelola melalui layer abstraksi yang menyembunyikan detail implementasi masing-masing

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

komponen dan menyediakan API yang koheren untuk aplikasi client.

F. Komponen Zero-Knowledge Proof

Untuk mengevaluasi model hibrid yang diusulkan, penelitian ini menggunakan setup eksperimental yang terdiri dari:

1. **Database**: PostgreSQL 14.0 dengan 5 GB data sintetis yang menyimulasikan database transaksional dengan informasi sensitif seperti data keuangan dan personal.
2. **Infrastructure**: Cluster Kubernetes dengan 10 node (masing-masing dengan 8 vCPU, 32 GB RAM) untuk menjalankan komponen blockchain, homomorphic encryption, dan zero-knowledge proof.
3. **Skenario Pengujian**: Simulasi 5 jenis serangan umum terhadap database:
   a. SQL Injection
   b. Man-in-the-Middle Attack
   c. Unauthorized Access Attempt
   d. Privilege Escalation
   e. Data Tampering
4. **Metrik Evaluasi**:
   a. Security Metrics: Detection rate, false positive rate, dan resistance score untuk masing-masing jenis serangan.
   b. Performance Metrics: Latency, throughput, dan resource utilization (CPU, memory, storage).
5. **Baseline Comparison**: Model hibrid yang diusulkan dibandingkan dengan 3 metode pengamanan database konvensional:
   a. Traditional encryption dengan access control
   b. Standalone blockchain-based auditing
   c. Database encryption dengan advanced access control

Prosedur Pengumpulan Data

Data dikumpulkan melalui eksperimen yang mensimulasikan lima jenis serangan umum: *SQL injection*, *man-in-the-middle*, *unauthorized access*, *privilege escalation*, dan *data tampering*. Setiap skenario diulang 100 kali. Model hibrid dibandingkan dengan tiga metode konvensional: *enkripsi* tradisional dengan ACL, *blockchain-only* auditing, dan *enkripsi* dengan ACL lanjutan.

Instrumen

Model hibrid mengintegrasikan tiga komponen: *blockchain*, *homomorphic encryption*, dan *zero-knowledge proof*. Komponen *blockchain* menggunakan *private blockchain* dengan algoritma konsensus Practical Byzantine Fault Tolerance (PBFT) yang dimodifikasi, mencatat aktivitas akses dan modifikasi. *Homomorphic encryption* menggunakan

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

skema Somewhat Homomorphic Encryption (SHE) berbasis Ring-Learning With Errors (Ring-LWE) dengan parameter: (1) derajat polinomial n = 4096, (2) modulus q = 2^{32}, dan (3) distribusi error χ = Gaussian diskrit dengan deviasi standar σ = 3.2. Komponen *zero-knowledge proof* menggunakan protokol zk-SNARK yang dioptimalkan dengan kurva eliptik BLS12-381, mencapai kompleksitas verifikasi O(1).

Teknik Analisis Data

Analisis statistik menggunakan uji-t dengan tingkat signifikansi α = 0,05 untuk membandingkan performa model hibrid dengan baseline. Metrik evaluasi meliputi *detection rate*, *false positive rate*, *resistance score*, *latency*, *throughput*, dan utilisasi sumber daya (CPU, memori, penyimpanan). Analisis kualitatif mengevaluasi kompleksitas implementasi dan *overhead* pemeliharaan.

HASIL DAN PEMBAHASAN

Efektivitas Keamanan

Model hibrid menunjukkan peningkatan signifikan dalam ketahanan terhadap berbagai serangan dibandingkan metode konvensional

Tabel 1. Detection Rate Comparison (%).

No	Jenis Serangan	Model Hibrid	Enkripsi Tradisional + ACL	Blockchain-only	Enkripsi + ACL Lanjutan
1	SQL Injection	99,7	78,3	82,1	85,4
2	Man-in-the-Middle	98,2	65,7	73,5	79,2
3	Uauthorized Access	100,0	89,5	95,2	94,8
4	Privilege Escalation	96,8	68,9	94,7	77,5
5	Data Tampering	99,9	68,9	94,7	77,5

Resistance score dihitung menggunakan rumus:

RS = (0,5 × DR) + (0,3 × (1 - FPR)) + (0,2 × CR) (1)

di mana RS adalah *resistance score*, DR adalah *detection rate*, FPR adalah *false positive rate*, dan CR adalah *containment rate*. Model hibrid mencapai *resistance score* rata-rata 95,8, dibandingkan 74,2, 83,5, dan 82,7 untuk baseline, menunjukkan keunggulan terutama terhadap *data tampering* (99,9%) dan *unauthorized access* (100%).

Performa Sistem

Tabel 2. Performance metrics comparison

No.	Metrik	Model Hibrid	Enkripsi Tradisional + ACL	Blockchain-only	Enkripsi + ACL Lanjutan
1	Latensi (ms)	185	24	142	58
2	Throughput (txn/s)	1250	8750	1.75	4,200
3	Utilisasi CPU (%)	68	25	52	37
4	Penggunaan Memori (GB)	12,4	3,8	9,2	5,6

Tabel 2 membandingkan metrik performa, menyoroti *trade-off* antara keamanan dan performa.Meskipun latensi meningkat 12% dibandingkan pendekatan *blockchain-only*, *throughput* 1.250 transaksi per detik masih

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

dapat diterima untuk aplikasi database perusahaan. Utilisasi CPU mencapai 68%, dengan penggunaan memori 12,4 GB dan *overhead* penyimpanan 47%.

Optimasi Zero-Knowledge Proof

Kontribusi utama adalah algoritma integrasi *zero-knowledge proof* yang dioptimalkan, mengurangi *overhead* komputasi sebesar 35% melalui teknik *batching* dan *paralelisasi*. Kompleksitas verifikasi turun dari O(n) menjadi O(log n), di mana n adalah jumlah *proof* yang diverifikasi.

Tabel 1. *Perbandingan Metrik Performa*

Integrasi Teknologi dan Sinergi

Model hibrid mengintegrasikan blockchain, homomorphic encryption, dan zero-knowledge proof untuk mengatasi kelemahan metode konvensional. *Blockchain* mencegah manipulasi *audit trail* (Wang et al., 2022). *Homomorphic encryption* menghilangkan kebutuhan penggunaan selama pemrosesan (Liu et al., 2022). *Zero-knowledge proof* memastikan verifikasi aman tanpa mengekspos kredensial (Sharma et al., 2022). Sinergi ini menciptakan mekanisme *defense-in-depth* yang komprehensif.

Trade-off Keamanan dan Performa

Model hibrid menawarkan peningkatan keamanan substansial dengan biaya latensi lebih tinggi dan *throughput* lebih rendah. Namun, *overhead* ini dapat diterima untuk aplikasi dengan data sensitif. Dibandingkan Ibrahim et al. (2023), optimasi yang diusulkan menghasilkan *overhead* performa lebih rendah untuk tingkat keamanan sebanding.

Keterbatasan Penelitian

Keterbatasan meliputi: 1. kompleksitas implementasi yang tinggi, 2. tantangan skalabilitas untuk database besar (>100 GB), 3. masalah kompatibilitas dengan sistem *legacy*, dan 4. tantangan manajemen kunci kriptografi.

SIMPULAN DAN SARAN

Penelitian ini mengusulkan model hibrid yang mengintegrasikan *blockchain*, *homomorphic encryption*, dan *zero-knowledge proof*, mencapai *detection rate* 99,7% untuk *SQL injection*, 98,2% untuk *man-in-the-middle*, dan 100% untuk *unauthorized access*. Meskipun latensi meningkat 12%, model ini menawarkan keseimbangan optimal untuk aplikasi data sensitif. Kontribusi utama adalah algoritma *zero-knowledge proof* yang dioptimalkan, mengurangi *overhead* komputasi sebesar 35%. Penelitian lanjutan disarankan untuk mengeksplorasi implementasi *federated*,

ISSN: XXXX-XXXX
e-ISSN: 2829-4459

varian tahan *quantum*, dan *governance* keamanan otomatis.

DAFTAR PUSTAKA

BSSN. (2023). Laporan Tahunan Keamanan Siber Indonesia 2023. Badan Siber dan Sandi Negara Indonesia.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, (2), 6-19.

Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University.

Goldwasser, S., Micali, S., & Rackoff, C. (2019). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), 186-208.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corp.

Ibrahim, K., Zhang, L., & Akbar, M. (2023). Secure DBaaS: Performance Analysis of Integrated Security Mechanisms for Database-as-a-Service. IEEE Transactions on Cloud Computing, 11(1), 312-325.

Liu, B., Zhu, L., & Zhang, Y. (2022). HEDB: A Database System with Homomorphic Encryption. IEEE Transactions on Dependable and Secure Computing, 19(2), 1108-1123.

Liu, H., Wang, D., & Zhang, C. (2023). Advanced Persistent Threats Against Database Systems: Taxonomy and Defense Mechanisms. ACM Transactions on Privacy and Security, 26(3), 1-35.

Rahman, A., Venkatraman, S., & Verma, R. (2023). Audit Trail Manipulation Techniques in Database Systems: Detection and Prevention. Journal of Computer Security, 31(2), 247-268.

Sharma, R., Kumar, A., & Patel, S. (2022). ZKP-Auth: An Efficient Zero-Knowledge Proof System for Database Authentication. Journal of Systems and Software, 185, 111223.

Sharma, S., & Chen, K. (2023). Bridging the Gap: Comprehensive Analysis of Database Encryption Techniques. IEEE Transactions on Information Forensics and Security, 18(2), 412-426.

Wang, X., Li, Y., Zhang, M., & Chen, L. (2022). BlockDBGuard: A Blockchain-Based Framework for Database Security and Access Control. IEEE Transactions on Knowledge and Data Engineering, 34(3), 1271-1285.