Jurnal Ilmu Komputer, Sistem Informasi, Teknik Informatika
ISSN: 2964-4763
Vol. 2, No. 2, September 2023

Implementasi Kriptografi Hibrida AES-256 dan ECC dengan Deteksi Anomali Berbasis Autoencoder untuk Keamanan Data Bisnis pada Infrastruktur Cloud Computing

Didik Setiayadi[1], Ribut Julianto[2], Cahya Ade Ningrum[3]
[123]Program Studi Informatika, Fakultas Sains dan Teknologi,
Universitas Indonesia Mandiri
Korespondensi: ributjulianto@uimandiri.ac.id

ABSTRAK

Adopsi infrastruktur cloud computing oleh sektor bisnis di Indonesia terus meningkat pesat, namun diiringi oleh eskalasi ancaman kebocoran data, akses tidak sah, dan serangan siber yang semakin canggih. Skema enkripsi tunggal berbasis AES atau RSA saja dinilai tidak lagi mencukupi untuk menghadapi lanskap ancaman modern yang memanfaatkan kelemahan pada lapisan kunci (key management) maupun pola akses anomali. Penelitian ini mengusulkan arsitektur keamanan data berlapis yang mengintegrasikan dua komponen utama: (1) skema kriptografi hibrida yang menggabungkan AES-256 untuk enkripsi data massal berkecepatan tinggi dengan Elliptic Curve Cryptography (ECC) kurva P-384 untuk manajemen kunci yang efisien dan aman, serta (2) model deteksi anomali akses berbasis Autoencoder deep learning yang mampu mengidentifikasi pola akses mencurigakan secara real-time tanpa memerlukan data berlabel. Sistem diimplementasikan pada lingkungan cloud AWS (Amazon Web Services) menggunakan infrastruktur multi-region dan diuji menggunakan dataset akses log dari tiga perusahaan sektor finansial dan manufaktur di Indonesia selama periode 12 bulan, mencakup 4,7 juta event akses. Hasil evaluasi menunjukkan: overhead enkripsi-dekripsi AES-256/ECC hanya sebesar 3,2% dibandingkan sistem tanpa enkripsi, model Autoencoder mencapai AUC-ROC 0,9712 dalam deteksi anomali akses dengan false positive rate 1,8%, dan sistem secara keseluruhan mampu memenuhi standar keamanan ISO/IEC 27001:2013 serta regulasi POJK No.11/2022 tentang Penyelenggaraan Teknologi Informasi oleh Lembaga Jasa Keuangan. Arsitektur yang diusulkan memberikan kerangka keamanan cloud yang komprehensif, efisien, dan dapat diadaptasi oleh pelaku industri di Indonesia.

Kata Kunci: *AES-256, ECC, Kriptografi Hibrida, Autoencoder, Deteksi Anomali*

ABSTRACT

The adoption of cloud computing infrastructure by the business sector in Indonesia continues to grow rapidly, accompanied by escalating threats of data breaches, unauthorized access, and increasingly sophisticated cyberattacks. Single encryption schemes based on AES or RSA alone are no longer sufficient to address the modern threat landscape that exploits weaknesses in key management layers and anomalous access patterns. This study proposes a layered data security architecture integrating two main components: (1) a hybrid cryptography scheme combining AES-256 for high-speed bulk data encryption with Elliptic Curve Cryptography (ECC) on curve P-384 for efficient and secure key management, and (2) an Autoencoder deep learning-based access anomaly detection model capable of identifying suspicious access patterns in real-time without requiring labeled data. The system was implemented on an AWS (Amazon Web Services) cloud environment using multi-region infrastructure and tested using access log datasets from three companies in Indonesia's financial and manufacturing sectors over a 12-month period, encompassing 4.7 million access events. Evaluation results show: AES-256/ECC encryption-decryption overhead of only 3.2% compared to unencrypted systems, the Autoencoder model achieves AUC-ROC of 0.9712 in access anomaly detection with a false positive rate of 1.8%, and the overall system meets ISO/IEC 27001:2013 security standards and OJK Regulation No. 11/2022 on IT Implementation by Financial Services Institutions. The proposed architecture provides a comprehensive, efficient, and adaptable cloud security framework for Indonesian industry practitioners.

Keywords: *AES-256, ECC, Hybrid Cryptography, Autoencoder, Anomaly Detection*

1. PENDAHULUAN

Cloud computing telah bertransformasi dari sekadar tren teknologi menjadi tulang punggung infrastruktur digital bisnis modern. Di Indonesia, laporan IDC Indonesia (2022) mencatat bahwa pengeluaran untuk layanan cloud publik mencapai USD 0,9 miliar pada tahun 2021 dan diproyeksikan tumbuh dengan CAGR 21,7% hingga tahun 2026. Sektor perbankan, asuransi, manufaktur, dan ritel menjadi adopter terbesar, memanfaatkan fleksibilitas, skalabilitas, dan efisiensi biaya yang ditawarkan oleh platform seperti AWS, Google Cloud Platform, dan Microsoft Azure.

Namun, perpindahan data bisnis sensitif ke lingkungan cloud membawa konsekuensi keamanan yang signifikan. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) Tahun 2022, terjadi lebih dari 274 juta anomali trafik siber di Indonesia sepanjang tahun 2021, dengan sektor keuangan dan bisnis menjadi

target utama. Insiden kebocoran data besar yang melibatkan data nasabah perbankan, data karyawan, dan data transaksi bisnis terus terjadi, menimbulkan kerugian finansial dan reputasional yang masif bagi perusahaan yang terdampak.

Tantangan keamanan cloud computing bersifat multidimensional. Dari aspek *data confidentiality*, data yang tersimpan dan ditransmisikan melalui infrastruktur cloud pihak ketiga memerlukan mekanisme enkripsi yang kuat agar tidak dapat dibaca oleh pihak yang tidak berwenang, termasuk administrator cloud provider sekalipun. Dari aspek *integrity* dan *availability*, sistem harus mampu mendeteksi dan merespons akses anomali serta percobaan intrusi secara real-time sebelum menimbulkan kerusakan. Regulasi seperti ISO/IEC 27001:2013, GDPR, dan secara spesifik untuk Indonesia yaitu POJK No.11/2022 dan UU Perlindungan Data Pribadi (PDP) No.27/2022 mewajibkan organisasi untuk mengimplementasikan kontrol teknis keamanan yang terukur dan terdokumentasi.

Skema kriptografi hibrida yang menggabungkan kriptografi simetris (*symmetric cryptography*) dan asimetris (*asymmetric cryptography*) menawarkan keseimbangan optimal antara kecepatan enkripsi dan keamanan manajemen kunci. AES-256 (Advanced Encryption Standard dengan kunci 256-bit) merupakan standar enkripsi simetris yang digunakan secara global dan telah disetujui oleh NIST sebagai standar federal AS, sementara ECC (Elliptic Curve Cryptography) memberikan tingkat keamanan yang setara dengan RSA-3072 namun dengan panjang kunci yang jauh lebih pendek (256-384 bit), menghasilkan komputasi yang lebih efisien — sangat relevan untuk lingkungan cloud dengan volume operasi kriptografi yang masif.

Di sisi deteksi ancaman, model Autoencoder berbasis deep learning menawarkan pendekatan yang efektif untuk deteksi anomali tanpa pengawasan (unsupervised anomaly detection) pada log akses cloud. Autoencoder dilatih untuk merekonstruksi pola akses normal, sehingga pola akses yang menyimpang secara signifikan dari pola normal akan menghasilkan reconstruction error yang tinggi dan dapat diidentifikasi sebagai anomali. Pendekatan ini sangat sesuai untuk konteks keamanan siber di mana pola serangan baru (zero-day attacks) tidak dapat diantisipasi sebelumnya melalui data berlabel.

Penelitian ini bertujuan: (1) merancang dan mengimplementasikan skema kriptografi hibrida AES-256/ECC untuk enkripsi data bisnis pada infrastruktur AWS multi-region, (2) mengembangkan model deteksi anomali akses berbasis Autoencoder yang dilatih pada data log akses normal, (3) mengevaluasi overhead performa sistem kriptografi terhadap throughput operasional, (4) membandingkan akurasi deteksi anomali dengan metode baseline, serta (5) memvalidasi kepatuhan sistem terhadap standar ISO/IEC 27001:2013 dan regulasi POJK No.11/2022.

2. TINJAUAN PUSTAKA

2.1 Keamanan Data pada Cloud Computing

Model layanan cloud computing mencakup tiga paradigma utama: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS). Masing-masing model memiliki implikasi keamanan yang berbeda terkait pembagian tanggung jawab (shared responsibility model) antara penyedia cloud dan pelanggan. Pada model IaaS seperti AWS EC2, pelanggan bertanggung jawab penuh atas keamanan sistem operasi, aplikasi, dan data, sementara provider hanya bertanggung jawab atas keamanan infrastruktur fisik.

Ancaman keamanan yang paling signifikan pada lingkungan cloud bisnis mencakup: data breaches akibat misconfiguration storage bucket (contoh: AWS S3 bucket yang terbuka publik), insider threats dari administrator cloud dengan hak akses berlebih, man-in-the-middle attacks pada transmisi data antar layanan cloud, serta credential stuffing dan brute-force attacks terhadap akun cloud. Laporan Verizon Data Breach Investigations Report (DBIR) 2022 mengidentifikasi bahwa 82% pelanggaran data melibatkan faktor manusia, baik melalui phishing, penggunaan kredensial yang dicuri, maupun kesalahan konfigurasi.

2.2 Kriptografi Hibrida: AES-256 dan ECC

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris blok (*block cipher*) yang beroperasi pada blok data 128-bit dengan panjang kunci 128, 192, atau 256 bit. Varian AES-256 dengan kunci 256-bit memberikan keamanan yang dianggap tidak dapat dipecahkan secara brute-force menggunakan komputasi klasik saat ini, bahkan mempertimbangkan proyeksi kapasitas komputasi kuantum jangka menengah. Mode operasi AES yang umum digunakan dalam konteks cloud adalah GCM (Galois/Counter Mode) yang menyediakan enkripsi terotentikasi (*Authenticated Encryption with Associated Data/AEAD*) yang secara simultan menjamin kerahasiaan dan integritas data.

Elliptic Curve Cryptography (ECC) merupakan pendekatan kriptografi kunci publik yang didasarkan pada struktur aljabar kurva eliptik atas medan hingga (*finite field*). Keunggulan fundamental ECC dibandingkan RSA terletak pada efisiensi komputasi: kurva P-384 (secp384r1) yang direkomendasikan NIST memberikan tingkat keamanan setara RSA-7680 bit, namun dengan ukuran kunci hanya 384 bit. Dalam skema kriptografi hibrida, ECC digunakan melalui protokol ECIES (*Elliptic Curve Integrated Encryption Scheme*) untuk mengenkripsi dan mendistribusikan kunci sesi AES secara aman antar pihak yang berkomunikasi, menghilangkan kebutuhan kanal distribusi kunci yang aman secara out-of-band.

2.3 Autoencoder untuk Deteksi Anomali

Autoencoder merupakan arsitektur neural network yang terdiri dari dua komponen: encoder yang memetakan input ke representasi laten berdimensi rendah (*bottleneck*), dan decoder yang merekonstruksi

input dari representasi laten tersebut. Model dilatih untuk meminimalkan *reconstruction error* (umumnya menggunakan Mean Squared Error) pada data latih yang hanya berisi pola normal. Pada fase inferensi, input yang memiliki pola jauh berbeda dari data latih normal akan menghasilkan reconstruction error yang tinggi — inilah yang dimanfaatkan sebagai sinyal anomali.

Untuk deteksi anomali pada log akses cloud, Variational Autoencoder (VAE) menawarkan keunggulan tambahan dibandingkan Autoencoder standar. VAE memaksakan representasi laten mengikuti distribusi Gaussian melalui *reparameterization trick*, menghasilkan ruang laten yang lebih terstruktur dan kontinu. Hal ini memungkinkan model untuk lebih robust dalam membedakan variasi normal dari anomali sejati, mengurangi false positive yang merupakan tantangan utama sistem deteksi intrusi dalam konteks operasional.

2.4 Penelitian Terdahulu

Subramanian dan Jeyaraj (2018) mengusulkan skema enkripsi hibrida RSA-AES untuk keamanan data pada cloud dan mengukur overhead performa pada berbagai ukuran file. Hasil penelitian menunjukkan overhead rata-rata 8,4% untuk AES-1024 bit RSA, namun tidak membahas aspek deteksi intrusi. Puthal et al. (2019) mengimplementasikan ECC untuk key management pada fog computing dan menunjukkan efisiensi energi 43% lebih baik dibandingkan RSA pada perangkat IoT.

Dari sisi deteksi anomali, Mirsky et al. (2018) mengembangkan Kitsune, sebuah sistem deteksi intrusi berbasis Autoencoder ensemble untuk traffic jaringan, mencapai AUC 0,98 pada berbagai skenario serangan. Di Indonesia, Pratama et al. (2022) menerapkan LSTM-Autoencoder untuk deteksi anomali pada log sistem ERP perusahaan manufaktur dengan AUC 0,9341. Celah penelitian yang belum tertangani adalah integrasi komprehensif antara skema kriptografi hibrida modern (AES-256/ECC) dengan deteksi anomali berbasis Autoencoder dalam satu arsitektur keamanan cloud terpadu untuk konteks bisnis Indonesia — yang menjadi kontribusi utama penelitian ini.

3. METODOLOGI PENELITIAN

3.1 Arsitektur Sistem Keamanan yang Diusulkan

Sistem yang diusulkan terdiri dari empat lapisan keamanan yang bekerja secara hierarkis dan terintegrasi:

- Lapisan Enkripsi Data (Data Encryption Layer): Implementasi AES-256-GCM untuk enkripsi data at-rest pada AWS S3 dan EBS, serta data in-transit melalui TLS 1.3 dengan cipher suite berbasis ECC (ECDHE-ECDSA-AES256-GCM-SHA384).

- Lapisan Manajemen Kunci (Key Management Layer): Protokol ECIES berbasis ECC P-384 untuk enkripsi dan distribusi kunci sesi AES. Kunci privat ECC disimpan menggunakan AWS KMS (Key Management Service) dengan Hardware Security Module (HSM) sebagai root of trust.
- Lapisan Deteksi Anomali (Anomaly Detection Layer): Model Variational Autoencoder yang memproses log akses cloud secara real-time melalui pipeline Apache Kafka, menghasilkan anomaly score untuk setiap event akses dalam waktu kurang dari 50 milidetik.
- Lapisan Respons dan Audit (Response & Audit Layer): Sistem notifikasi otomatis melalui AWS SNS untuk event dengan anomaly score di atas threshold, dashboard monitoring berbasis Grafana, dan audit trail terenkripsi yang disimpan di AWS CloudTrail.

3.2 Dataset dan Lingkungan Implementasi

Penelitian ini menggunakan dua jenis data utama:

a) Dataset Log Akses Cloud

Data log akses dari sistem cloud tiga perusahaan mitra (dianonimkan sebagai Perusahaan A — sektor perbankan, Perusahaan B — asuransi, Perusahaan C — manufaktur) yang dikumpulkan selama 12 bulan (Januari–Desember 2022). Total 4,7 juta event akses dengan distribusi sebagai berikut:

Perusahaan	Total Event	Event Normal	Event Anomali	Layanan Cloud
Perusahaan A (Bank)	2.134.872	2.098.341	36.531 (1,7%)	AWS EC2, RDS, S3
Perusahaan B (Asuransi)	1.487.233	1.461.109	26.124 (1,8%)	AWS Lambda, DynamoDB
Perusahaan C (Manufaktur)	1.078.415	1.054.872	23.543 (2,2%)	AWS ECS, Aurora
Total	4.700.520	4.614.322	86.198 (1,8%)	Multi-service AWS

Tabel 1. Distribusi Dataset Log Akses Cloud

b) Dataset Enkripsi Performa

Dataset sintetis berisi file dengan berbagai ukuran (1 KB hingga 1 GB) yang digunakan untuk mengukur overhead performa operasi kriptografi AES-256 dan ECC. Total 50.000 operasi enkripsi-dekripsi dilakukan pada instance AWS EC2 t3.xlarge (4 vCPU, 16 GB RAM) untuk memperoleh statistik performa yang representatif.

3.3 Implementasi Kriptografi Hibrida AES-256/ECC

Alur kerja kriptografi hibrida yang diimplementasikan mengikuti protokol berikut:

1. Key Generation: Setiap entitas (user/service) memiliki pasangan kunci ECC P-384 yang dibangkitkan menggunakan Cryptographically Secure Pseudo-Random Number Generator (CSPRNG). Kunci privat disimpan terenkripsi di AWS KMS dengan envelope encryption.

2. Session Key Derivation: Untuk setiap sesi enkripsi, kunci sesi AES-256 (32 byte) dibangkitkan secara acak. Kunci sesi ini kemudian dienkripsi menggunakan ECIES dengan kunci publik ECC penerima, menghasilkan ciphertext kunci yang aman untuk transmisi.
3. Data Encryption: Data aktual dienkripsi menggunakan AES-256-GCM dengan kunci sesi yang telah dibangkitkan. Mode GCM menghasilkan authentication tag 128-bit yang menjamin integritas dan keaslian data secara bersamaan.
4. Transmission: Paket terenkripsi terdiri dari: ECIES-encrypted session key + AES-GCM ciphertext + GCM authentication tag + initialization vector (IV) 96-bit yang unik untuk setiap operasi enkripsi.
5. Decryption: Penerima mendekripsi kunci sesi menggunakan kunci privat ECC-nya, kemudian mendekripsi data menggunakan kunci sesi yang dipulihkan, sekaligus memverifikasi authentication tag untuk memastikan integritas data.

3.4 Arsitektur Model Variational Autoencoder

Komponen	Layer Detail	Aktivasi	Output Dim
Input Layer	– (fitur log akses)	–	128
Encoder FC-1	Dense 128 → 64 + BatchNorm	ReLU	64
Encoder FC-2	Dense 64 → 32 + Dropout(0.2)	ReLU	32
Latent Space (μ, σ)	Dense 32 → 16 (mean & log-var)	Linear	16
Decoder FC-1	Dense 16 → 32 + BatchNorm	ReLU	32
Decoder FC-2	Dense 32 → 64 + Dropout(0.2)	ReLU	64
Output Layer	Dense 64 → 128	Sigmoid	128

Tabel 2. Arsitektur Variational Autoencoder untuk Deteksi Anomali

Model VAE dilatih menggunakan data log akses normal selama 10 bulan pertama (80% training, 20% validation), sementara 2 bulan terakhir digunakan sebagai test set yang mencakup event anomali yang telah diverifikasi secara manual oleh tim keamanan perusahaan mitra. Loss function yang digunakan adalah kombinasi antara reconstruction loss (Binary Cross-Entropy) dan KL-divergence regularization term yang merupakan karakteristik khas VAE.

3.5 Feature Engineering Log Akses

Dari setiap event log akses AWS CloudTrail, diekstraksi 128 fitur yang dikelompokkan dalam lima kategori:

- Fitur Identitas (24 fitur): User ARN, peran IAM, jenis autentikasi (password/MFA/role assumption), flag akses lintas akun, jumlah permission yang digunakan per sesi.

- Fitur Temporal (18 fitur): Jam akses, hari kerja/libur, selisih waktu dari akses sebelumnya, frekuensi akses per jam/hari/minggu, flag akses di luar jam kerja.
- Fitur Jaringan (22 fitur): Alamat IP sumber, geolokasi (negara, kota, ASN), flag VPN/Tor/proxy, reputasi IP dari threat intelligence feed, jenis koneksi (direct/VPC/endpoint).
- Fitur Resource (32 fitur): Jenis layanan AWS yang diakses, jenis operasi API (read/write/delete/admin), sensitivity level resource, volume data yang diakses atau dimodifikasi per sesi.
- Fitur Behavioral (32 fitur): Pola akses historis 7/30/90 hari terakhir per user, deviasi dari baseline perilaku normal, jumlah API call gagal, perubahan konfigurasi keamanan.

3.6 Konfigurasi Training dan Threshold Anomali

Parameter	Konfigurasi
Framework	TensorFlow 2.13 + Keras
Optimizer	Adam (lr=0.001, β_1=0.9, β_2=0.999)
Loss Function	BCE Reconstruction Loss + β-KL Divergence (β=4)
Batch Size	512
Epoch	200 dengan Early Stopping (patience=15)
Threshold Anomali	Persentil ke-99 dari reconstruction error pada validation set
Hardware	AWS p3.2xlarge (NVIDIA V100 16GB)
Inferensi Real-time	Apache Kafka + TensorFlow Serving (< 50 ms/event)

Tabel 3. Konfigurasi Training Model VAE

4. HASIL DAN PEMBAHASAN

4.1 Performa Kriptografi Hibrida AES-256/ECC

Ukuran Data	Throughput AES	Throughput ECC	Throughput Hibrida	Throughput Plaintext	Overhead (%)
1 KB	487 MB/s	312 MB/s	298 MB/s	312 MB/s	4,5%
1 MB	512 MB/s	–	509 MB/s	524 MB/s	2,9%
100 MB	518 MB/s	–	516 MB/s	531 MB/s	2,8%
1 GB	521 MB/s	–	519 MB/s	536 MB/s	3,2%
Rata-rata	–	–	–	–	3,2%

Tabel 4. Perbandingan Throughput Kriptografi pada Instance AWS EC2 t3.xlarge

Hasil pengukuran menunjukkan bahwa overhead rata-rata sistem kriptografi hibrida AES-256/ECC hanya sebesar 3,2% dibandingkan operasi tanpa enkripsi. Angka ini jauh di bawah threshold toleransi umum industri sebesar 10%, mengkonfirmasi kelayakan implementasi sistem ini dalam lingkungan produksi dengan beban kerja tinggi. Penggunaan instruksi hardware AES-NI (AES New Instructions) yang tersedia

pada prosesor Intel Xeon generasi terbaru yang digunakan oleh AWS EC2 menjadi faktor utama efisiensi ini. Overhead yang lebih tinggi pada file kecil (1 KB, 4,5%) disebabkan oleh operasi ECC untuk pertukaran kunci yang memiliki biaya komputasi relatif tetap dan lebih terasa signifikan pada data berukuran kecil.

Metrik	RSA-2048/AES-256	RSA-4096/AES-256	ECC-P384/AES-256 (Ours)	Keunggulan Ours
Ukuran Kunci Publik	256 bytes	512 bytes	97 bytes	↓ 62% vs RSA-2048
Waktu Key Gen.	4,2 ms	47,8 ms	1,1 ms	↓ 73,8% vs RSA-2048
Waktu Sign/Verify	1,8 / 2,1 ms	14,2 / 16,8 ms	0,9 / 1,2 ms	↓ 50% vs RSA-2048
Equivalent Security	~112 bit	~140 bit	~192 bit	Tertinggi
Overhead Memori	48 KB	96 KB	24 KB	↓ 50% vs RSA-2048

Tabel 5. Perbandingan ECC P-384 dengan Skema RSA untuk Key Management

Perbandingan antara ECC P-384 dan RSA untuk komponen manajemen kunci menunjukkan keunggulan signifikan ECC pada seluruh metrik yang diukur. Ukuran kunci publik yang 62% lebih kecil dari RSA-2048 memiliki implikasi praktis penting dalam konteks cloud computing: pengurangan overhead jaringan pada transmisi sertifikat digital, pengurangan kebutuhan penyimpanan dalam sistem Public Key Infrastructure (PKI), dan peningkatan kecepatan operasi TLS handshake yang terjadi ribuan kali per detik pada server API cloud.

4.2 Performa Deteksi Anomali VAE

Model	Precision	Recall	F1-Score	AUC-ROC	FPR (%)
Statistical (Z-Score)	0.6234	0.7891	0.6963	0.8234	12,4%
Isolation Forest	0.7812	0.8234	0.8018	0.9134	6,8%
One-Class SVM	0.7341	0.7967	0.7641	0.8923	8,2%
LSTM-Autoencoder	0.8512	0.8734	0.8621	0.9512	4,3%
Standard AE	0.8734	0.8912	0.8822	0.9634	3,2%
VAE (Ours)	0.9012	0.9134	0.9073	0.9712	1,8%

Tabel 6. Perbandingan Performa Model Deteksi Anomali Akses Cloud

Model VAE yang diusulkan secara konsisten mengungguli seluruh model pembanding pada semua metrik. Penurunan False Positive Rate (FPR) dari 3,2% (Standard AE) menjadi 1,8% (VAE) merupakan peningkatan yang sangat signifikan dalam konteks operasional. Pada volume log 4,7 juta event, perbedaan 1,4 poin FPR berarti pengurangan sekitar 65.800 alert palsu yang harus ditangani oleh tim keamanan — setara dengan penghematan ratusan jam kerja analis keamanan per tahun.

4.3 Evaluasi Kepatuhan Regulasi

Kontrol Regulasi	Standar / Regulasi	Status Pemenuhan
Enkripsi Data at Rest	ISO 27001:2013 A.10.1, POJK 11/2022 Ps.15	✓ AES-256-GCM Implemented
Enkripsi Data in Transit	ISO 27001:2013 A.10.1, UU PDP Ps.35	✓ TLS 1.3 + ECC Cipher Suite
Manajemen Kunci Kriptografi	ISO 27001:2013 A.10.1.2, NIST SP 800-57	✓ AWS KMS + HSM Root of Trust
Deteksi & Monitoring Anomali	ISO 27001:2013 A.12.4, POJK 11/2022 Ps.29	✓ VAE Real-time (< 50 ms)
Audit Trail & Log Retention	ISO 27001:2013 A.12.4.1, POJK 11/2022 Ps.31	✓ AWS CloudTrail + Encrypted S3
Pemulihan Bencana (RTO/RPO)	ISO 27001:2013 A.17, POJK 11/2022 Ps.40	✓ Multi-region AWS (RTO<15m)

Tabel 7. Pemetaan Sistem terhadap Standar Keamanan dan Regulasi

Validasi kepatuhan regulasi dilakukan melalui assessment terstruktur yang mengacu pada control objectives ISO/IEC 27001:2013 dan persyaratan teknis POJK No.11/2022. Hasil assessment menunjukkan bahwa seluruh enam domain kontrol keamanan yang diuji berhasil dipenuhi oleh arsitektur sistem yang diusulkan. Ini menjadikan sistem layak diimplementasikan oleh lembaga jasa keuangan (LJK) di Indonesia yang wajib mematuhi regulasi OJK terkait penyelenggaraan teknologi informasi.

4.4 Analisis Jenis Anomali yang Terdeteksi

Dari 86.198 event anomali yang terverifikasi dalam dataset, model VAE berhasil mendeteksi 78.743 event (recall 91,3%). Distribusi jenis anomali yang berhasil diidentifikasi adalah sebagai berikut: (1) akses dari geolokasi tidak biasa / impossible travel (32,4%), (2) operasi API sensitif di luar jam kerja (27,8%), (3) volume data download/exfiltration yang melebihi baseline (18,9%), (4) percobaan akses ke resource tidak berwenang berulang (12,7%), dan (5) pola credential stuffing dan brute-force (8,2%). Temuan ini mengkonfirmasi bahwa insider threat dan akses dari akun yang dikompromikan merupakan ancaman dominan yang perlu diprioritaskan dalam strategi keamanan cloud bisnis.

4.5 Pembahasan Implikasi Bisnis dan Operasional

Dari perspektif bisnis, implementasi sistem yang diusulkan memberikan nilai terukur pada beberapa dimensi. Pertama, reduksi risiko finansial: berdasarkan laporan IBM Cost of a Data Breach 2022, rata-rata biaya kebocoran data di Asia Pasifik mencapai USD 2,87 juta per insiden. Dengan recall deteksi anomali 91,3% dan waktu deteksi rata-rata kurang dari 50 milidetik, sistem memungkinkan respons insiden yang jauh lebih cepat dibandingkan rata-rata waktu deteksi konvensional yang mencapai 207 hari (DBIR 2022).

Kedua, kepatuhan regulasi: terpenuhinya persyaratan POJK No.11/2022 mengeliminasi risiko sanksi administratif yang dapat mencapai Rp 15 miliar untuk pelanggaran keamanan data oleh LJK.

Overhead performa 3,2% dari implementasi kriptografi hibrida memiliki implikasi biaya cloud yang minimal. Pada instance AWS EC2 t3.xlarge dengan biaya USD 0,1664/jam, overhead 3,2% setara dengan tambahan biaya sekitar USD 0,005/jam — nilai yang sangat kecil dibandingkan nilai perlindungan data bisnis yang dijamin. Skalabilitas sistem pada arsitektur AWS multi-region memastikan bahwa overhead ini tetap konstan bahkan pada peningkatan beban kerja yang signifikan, berkat dukungan hardware AES-NI pada seluruh jenis instance EC2 generasi terkini.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini berhasil merancang, mengimplementasikan, dan mengevaluasi arsitektur keamanan cloud berlapis yang mengintegrasikan kriptografi hibrida AES-256/ECC dengan deteksi anomali berbasis Variational Autoencoder. Kesimpulan utama yang dapat ditarik adalah:

- Skema kriptografi hibrida AES-256-GCM/ECC P-384 memberikan overhead performa hanya 3,2% dibandingkan sistem tanpa enkripsi, jauh di bawah threshold toleransi industri 10%, dengan tingkat keamanan ekivalen RSA-7680 bit menggunakan ukuran kunci 62% lebih kecil dari RSA-2048.
- Model Variational Autoencoder mencapai AUC-ROC 0,9712 dan False Positive Rate hanya 1,8% dalam deteksi anomali akses cloud, mengungguli lima model baseline termasuk Isolation Forest, One-Class SVM, LSTM-Autoencoder, dan Standard Autoencoder.
- Penurunan FPR dari 3,2% (Standard AE) menjadi 1,8% (VAE) berarti pengurangan 65.800 false alert per 4,7 juta event, setara penghematan ratusan jam kerja analis keamanan per tahun.
- Sistem berhasil memenuhi seluruh enam domain kontrol keamanan yang diuji berdasarkan ISO/IEC 27001:2013 dan POJK No.11/2022, menjadikannya layak diimplementasikan oleh lembaga jasa keuangan yang diawasi OJK.
- Waktu inferensi deteksi anomali di bawah 50 milidetik per event memungkinkan respons insiden yang real-time, secara signifikan memangkas window of exposure dibandingkan metode deteksi konvensional.

5.2 Saran

6. Eksplorasi integrasi algoritma Post-Quantum Cryptography (PQC) seperti CRYSTALS-Kyber yang sedang dalam proses standardisasi NIST (NIST PQC Round 3, 2022) sebagai lapisan keamanan tambahan untuk mengantisipasi ancaman komputasi kuantum jangka panjang.
7. Pengembangan model VAE yang dapat melakukan continual learning secara inkremental terhadap pola akses baru tanpa perlu retraining penuh, menggunakan teknik Elastic Weight Consolidation (EWC) untuk mengatasi catastrophic forgetting.
8. Penelitian lanjutan tentang implementasi Homomorphic Encryption untuk memungkinkan komputasi pada data terenkripsi di cloud tanpa dekripsi, mengeliminasi risiko exposure data pada layer pemrosesan.

9. Pengembangan dataset benchmark log akses cloud spesifik Indonesia yang dapat dipublikasikan untuk keperluan penelitian, mengingat keterbatasan dataset publik yang mencerminkan karakteristik penggunaan cloud di Indonesia.

DAFTAR PUSTAKA

[1] NIST. (2001). Advanced Encryption Standard (AES). Federal Information Processing Standard Publication 197. National Institute of Standards and Technology.

[2] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209.

[3] Kingma, D. P., & Welling, M. (2013). Auto-encoding variational bayes. arXiv preprint arXiv:1312.6114.

[4] Subramanian, G., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28–42.

[5] Puthal, D., Ranjan, R., Nanda, A., Nanda, P., Jayaraman, P. P., & Chen, J. (2019). Secure authentication and load balancing of distributed edge datacenters. Journal of Parallel and Distributed Computing, 124, 60–69.

[6] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. Proceedings of NDSS 2018.

[7] Pratama, R., Sari, C. A., & Setiadi, D. R. I. M. (2022). Deteksi anomali pada sistem ERP berbasis LSTM-Autoencoder. Jurnal Teknologi dan Sistem Komputer, 10(3), 145–153.

[8] Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). Verizon Business.

[9] IBM Security. (2022). Cost of a Data Breach Report 2022. IBM Corporation.

[10] ISO/IEC. (2013). ISO/IEC 27001:2013 — Information Technology — Security Techniques — Information Security Management Systems — Requirements. International Organization for Standardization.

[11] OJK. (2022). Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Jakarta: Otoritas Jasa Keuangan.

[12] BSSN. (2022). Laporan Tahunan BSSN 2021: Lanskap Keamanan Siber Indonesia. Jakarta: Badan Siber dan Sandi Negara.

[13] NIST. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (NISTIR 8413). National Institute of Standards and Technology.

[14] Hawkins, D. M. (1980). Identification of Outliers. Chapman and Hall, London.

[15] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems (NeurIPS), 30.