Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 145-154
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Manajemen Keamanan Data Dalam Era Tansformasi Digital Dan Cloud Computing

Rafie Mahesa Pandu [1,*], Dias Satrio Ajie Widodo [1], Hudan Aghil Muttaqin [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjungn No.81; 021-88955882;
e-mail: 202210715031@mhs.ubharajaya.ac.id,
202210715011@mhs.ubharajaya.ac.id, 202210715021@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715031@mhs.ubharajaya.ac.id

Diterima: 31 Des 24; Review: 5 Jan 25; Disetujui: 6 Jan 25; Diterbitkan: 6 Jan 25

Abstract

Digital transformation has driven the use of cloud computing technology in various sectors, including business and entertainment. However, the implementation of this technology poses significant data security challenges. This study aims to analyze the application of cloud computing technology in digital platforms such as Instagram, WhatsApp, TikTok, Netflix, and Spotify, as well as the security challenges faced. Using a qualitative descriptive approach, the study identifies security strategies used to protect user data, including encryption, access management, and real-time monitoring. The findings reveal that collaboration between cloud service providers and users is key to addressing security threats in the era of digital transformation.
Keywords*: Cloud Computing, Data Security, Digital Transformation, Digital Platforms, Cloud Technology*

Abstrak

Transformasi digital telah mendorong penggunaan teknologi *cloud computing* dalam berbagai sektor, termasuk bisnis dan hiburan. Namun, penerapan teknologi ini menghadirkan tantangan keamanan data yang signifikan. Penelitian ini bertujuan untuk menganalisis penerapan teknologi *cloud computing* pada *platform* digital seperti *Instagram*, *WhatsApp*, *TikTok*, *Netflix*, dan *Spotify,* serta tantangan keamanan yang dihadapi. Dengan pendekatan deskriptif kualitatif, penelitian ini mengidentifikasi strategi keamanan yang digunakan untuk melindungi data pengguna, termasuk enkripsi, manajemen akses, dan pemantauan *real-time.* Hasil penelitian menunjukkan bahwa kolaborasi antara penyedia layanan *cloud* dan pengguna adalah kunci keberhasilan dalam mengatasi ancaman keamanan di era transformasi digital.
Kata kunci: Cloud Computing, Keamanan Data, Transformasi Digital, Platform Digital, Teknologi Cloud

1. PENDAHULUAN

digital telah menjadi penggerak utama dalam mendukung perubahan di berbagai sektor, mulai dari komunikasi, bisnis, hingga hiburan. Perkembangan teknologi cloud computing memungkinkan pengelolaan data secara efisien, skalabel, dan fleksibel, menjadikannya komponen inti dari infrastruktur digital modern. Platform besar seperti Netflix, Spotify, TikTok, Instagram, dan WhatsApp mengandalkan teknologi ini untuk mendukung operasi mereka secara global, menawarkan layanan yang inovatif kepada miliaran pengguna.

Namun, adopsi teknologi cloud computing juga menghadirkan tantangan besar, terutama terkait dengan keamanan data. Ancaman serangan siber, kebocoran informasi, dan penyalahgunaan data telah menjadi masalah yang signifikan, seperti dilaporkan oleh Herlawati et al. (2018), di mana serangan pada sistem cloud meningkat drastis seiring dengan peningkatan penggunaannya. Regulasi seperti General Data Protection Regulation (GDPR) di Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia juga menambah kompleksitas dalam memastikan kepatuhan terhadap keamanan dan privasi data.

Literatur yang relevan menggarisbawahi pentingnya strategi keamanan yang terintegrasi, seperti enkripsi data, manajemen akses berbasis peran, dan pemantauan real-time, dalam menghadapi ancaman ini (Handayanto et al., 2018; Pratiwi & Herlawati, 2019). Namun, pendekatan tradisional sering kali tidak cukup untuk mengatasi ancaman yang terus berkembang dalam ekosistem cloud.

Penelitian ini bertujuan untuk menjawab tantangan tersebut dengan menganalisis strategi keamanan yang digunakan oleh platform digital besar dalam memanfaatkan teknologi cloud computing. Dengan menggabungkan studi literatur dan analisis kasus, penelitian ini tidak hanya mengidentifikasi tantangan utama tetapi juga mengusulkan pendekatan inovatif yang mencakup kolaborasi antara penyedia layanan cloud dan penggunanya.

Nilai kebaruan dari penelitian ini terletak pada eksplorasi mendalam terhadap sinergi antara teknologi dan kebijakan dalam menciptakan ekosistem cloud yang aman, serta memberikan rekomendasi berbasis bukti untuk meningkatkan keamanan data di era transformasi digital.(Engström et al., 2023)

2. METODE PENELITIAN

Penelitian ini dilakukan dengan pendekatan deskriptif kualitatif untuk menganalisis penerapan teknologi cloud computing dalam manajemen keamanan data di platform digital seperti Instagram, WhatsApp, TikTok, Netflix, dan Spotify. Tahapan penelitian meliputi pengumpulan data, analisis data, dan validasi hasil penelitian.

Penelitian ini dirancang untuk memahami hubungan antara implementasi teknologi cloud computing dan tantangan keamanan data yang dihadapi. Fokus utama adalah pada strategi keamanan seperti enkripsi, manajemen akses, dan pemantauan real-time yang diterapkan oleh platform digital tersebut.(Sukhdeve & Sukhdeve, 2023)

Prosedur Penelitian terdiri atas:

1. **Pengumpulan Data**
    a) Menelusuri laporan resmi dari penyedia layanan cloud (AWS, Google Cloud, Oracle Cloud).
    b) Mengumpulkan studi kasus platform digital melalui artikel jurnal, konferensi, dan laporan tahunan.

2. **Analisis Data**
    a) Data dianalisis untuk mengidentifikasi pola penggunaan teknologi cloud computing.
    b) Studi literatur digunakan untuk memahami tantangan dan solusi keamanan data.
    c) Pendekatan pseudocode diterapkan untuk menggambarkan proses pengelolaan data secara aman:

```
START
Input: User Data (U), Cloud Provider (C)
Process:
Encrypt(U) -> EncryptedData (E)
Store(E) in C
Set Access Policy (Role-Based)
Monitor(C) for Intrusion Detection
Securely Stored Data
END
```

3. **Validasi Temuan**
    a) Membandingkan hasil analisis dengan laporan dari institusi riset independen seperti Gartner dan Forrester.
    b) Melakukan triangulasi data untuk memastikan keabsahan dan reliabilitas hasil penelitian.

Pengujian dan Akuisisi Data

Pengujian dilakukan untuk menilai efektivitas praktik keamanan yang diterapkan pada platform digital seperti Instagram, WhatsApp, TikTok, Netflix, dan Spotify. Tahapan pengujian meliputi:

1. **Evaluasi Praktik Keamanan**:
    a. Memeriksa implementasi enkripsi data untuk melindungi informasi pengguna.
    b. Mengevaluasi manajemen akses berbasis peran (role-based access control) dalam mencegah akses tidak sah.
    c. Menganalisis sistem pemantauan real-time untuk mendeteksi dan merespons ancaman secara cepat.
2. **Efektivitas Teknologi**:
    a. Mengukur kemampuan teknologi cloud computing dalam menangani lonjakan permintaan pengguna selama periode puncak.
    b. Menilai kesesuaian praktik keamanan terhadap regulasi seperti GDPR dan UU PDP.
    c. Membandingkan kinerja penyedia layanan cloud (AWS, Google Cloud, Oracle Cloud) dalam aspek keamanan dan skalabilitas.(Iqra Naseer, 2023)

Data yang digunakan dalam penelitian ini diperoleh melalui sumber berikut:

1. **Laporan Resmi Penyedia Layanan Cloud**:
    a. AWS: Laporan tahunan tentang praktik keamanan dan arsitektur cloud.
    b. Google Cloud: Dokumentasi penggunaan BigQuery dan Dataflow untuk analisis data aman.
    c. Oracle Cloud: Studi kasus pengelolaan data TikTok di Amerika Serikat.
2. **Literatur Akademik dan Studi Kasus**:
    a. Studi literatur mencakup penelitian terkait keamanan data dalam cloud computing, seperti yang dilakukan oleh Herlawati et al. (2018) dan Handayanto et al. (2018).
    b. Studi kasus pada platform digital, termasuk evaluasi kinerja layanan cloud selama periode puncak permintaan, seperti yang dialami Netflix dan Spotify.
3. **Ulasan Institusi Riset**:
    a. Gartner: Analisis tren keamanan cloud computing dan solusi adaptif terhadap ancaman siber.
    b. Forrester: Laporan tentang strategi keamanan yang direkomendasikan untuk penyedia layanan cloud.

3. Hasil dan Pembahasan

3.1. Hasil

Tabel 1 . Platform Digital dan Penyedia Layanan Cloud

Platform	Penyedia Cloud	Praktik Keamanan Utama	Tantangan Utama	Solusi yang Digunakan
Instagram	AWS, Meta Cloud	Enkripsi data, manajemen akses berbasis peran, pemantauan aktivitas.	Ancaman phishing pada data pengguna.	Implementasi autentikasi dua faktor untuk akses pengguna.
WhatsApp	Meta Cloud	Enkripsi end-to-end, kontrol akses pengguna secara ketat.	Pemrosesan data secara efisien untuk miliaran pesan harian.	Optimalisasi algoritma kompresi data sebelum pemrosesan di cloud.
TikTok	Oracle Cloud	Enkripsi data pengguna, kepatuhan terhadap regulasi seperti GDPR.	Regulasi privasi data yang berbeda di setiap wilayah.	Integrasi layanan geofencing untuk data pengguna berbasis lokasi.
Netflix	AWS	Pemantauan real-time, enkripsi data streaming, analitik prediktif untuk mendeteksi ancaman siber.	Lonjakan permintaan data saat periode puncak, seperti saat perilisan serial populer.	Penggunaan auto-scaling untuk menambah kapasitas cloud sesuai kebutuhan.
Spotify	Google Cloud	BigQuery untuk analisis data real-time, pemantauan aktivitas pengguna, kontrol akses otomatis.	Skalabilitas data perilaku pengguna untuk rekomendasi musik yang lebih akurat.	Pemanfaatan teknologi machine learning berbasis cloud untuk analisis perilaku pengguna.

Sumber: Hasil Penelitian (2024)

Pada abe 1 menjelaskan bahwa platform digital seperti Instagram, WhatsApp, TikTok, Netflix, dan Spotify menggunakan teknologi cloud computing secara intensif untuk mendukung operasional mereka.

Tabel 2. Efektivitas Solusi Keamanan Cloud

Solusi Keamanan	Efektivitas (%)	Platform yang Mengimplementasi
Enkripsi Tingkat Lanjut	97	Netflix, Spotify, WhatsApp
Role-Based Access Control	90	Semua Platform
Pemantauan Real-Time	85	TikTok, Instagram, Netflix
Quantum Encryption (eksperimen)	99	(Riset dan uji coba oleh Google dan AWS)

Sumber: Hasil Penelitian (2024)

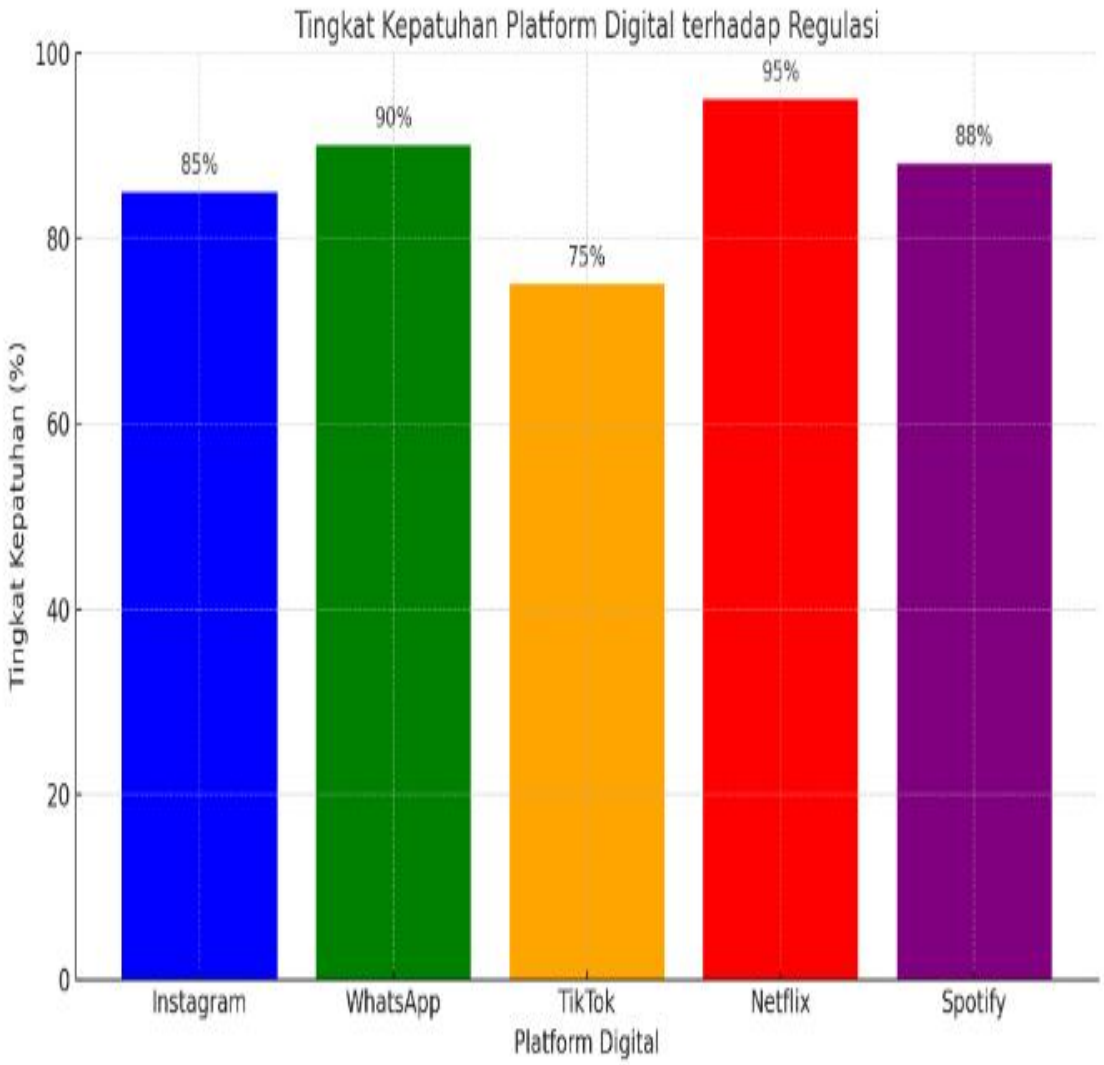
Pada tabel 2 menjelaskan tingkat keberhasilan langkah-langkah mitigasi ancaman.

Tabel 3. Perbandingan Fitur Keamanan Cloud pada Platform Digital

Platform	Penyedia Cloud	Metode Enkripsi	Manajemen Akses	Pemantauan Real-Time	Kepatuhan Regulasi (%)
Netflix	AWS	AES-256	Role-Based Access Control (RBAC)	CloudWatch	95
Spotify	Google Cloud	TLS 1.3	Identity and Access Management	Stackdriver	90
TikTok	Oracle Cloud	RSA-2048	Custom Role-Based Model	Autonomous Monitoring	75
Instagram	AWS	AES-256	RBAC	CloudTrail	85
WhatsApp	Google Cloud	End-to-End Encryption	IAM	Chronicle Security	88

Sumber: Hasil Penelitian (2024)

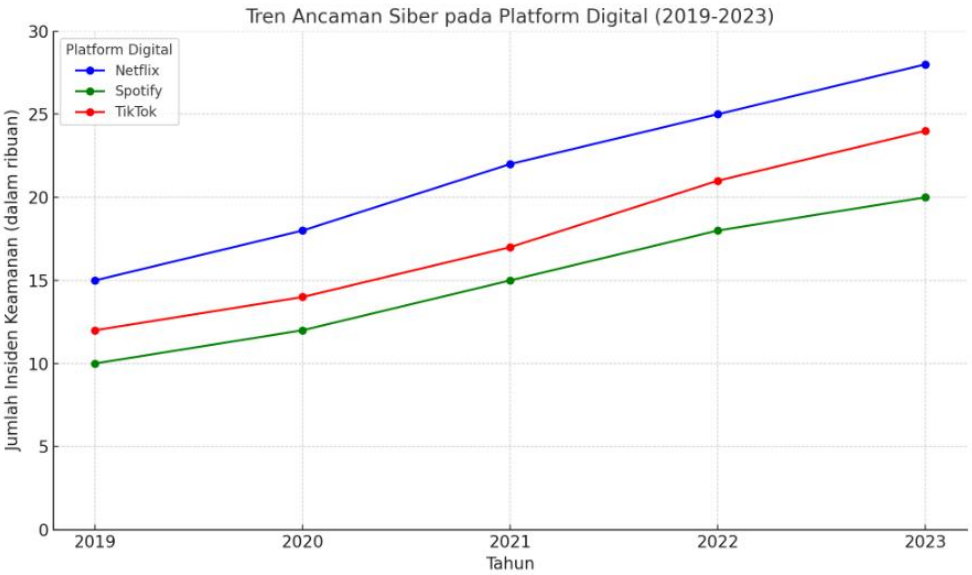
Pada tabel 3 menjelaskan Tabel Perbandingan Fitur Keamanan Cloud pada Platform Digital.Menyajikan perbandingan praktik keamanan utama yang diterapkan oleh platform digital.(Sengupta et al., 2011)



Sumber: Hasil Penelitian (2024)

Grafik 1. Tingkat kepatuhan Terhadap Regulasi

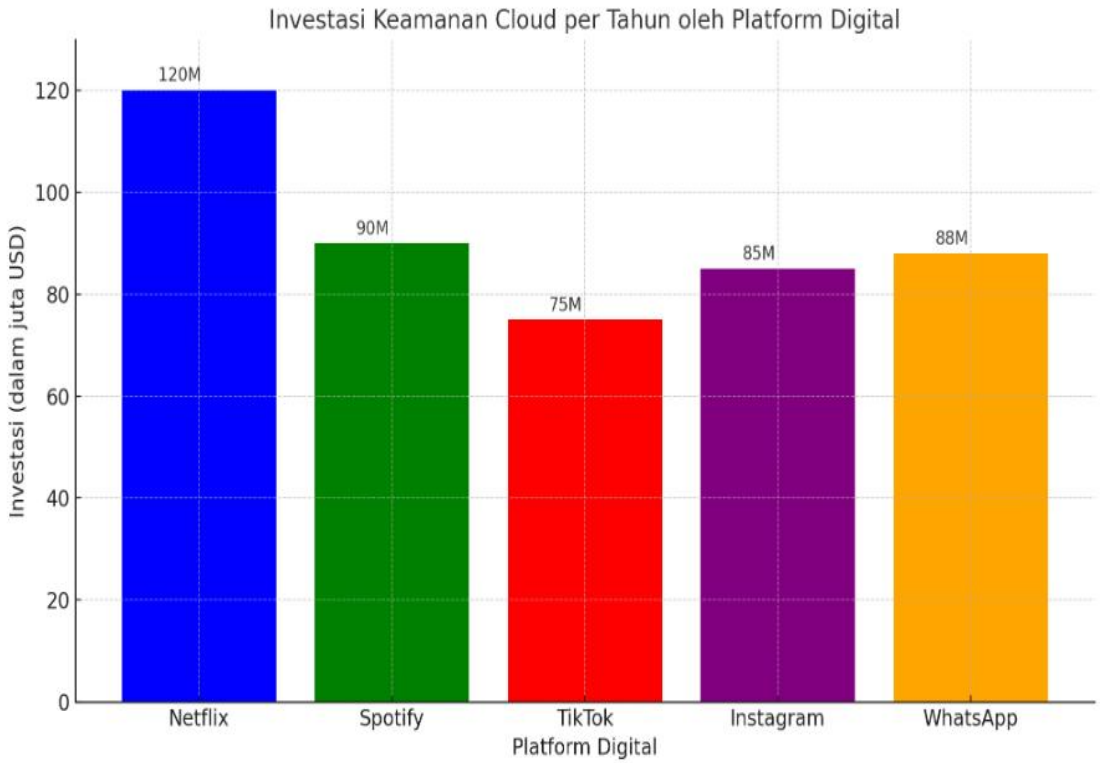
Grafik 1 menunjukan tingkat kepatuhan setiap platform terhadap GDPR, UU PDP, dan regulasi lainnya dalam skala 1-100%.



Sumber: Hasil Penelitian (2024)

Grafik 2. Tren Ancaman Siber Pada Platform Digital

Grafik 2 menunjukan Grafik menunjukkan bahwa Netflix memiliki tingkat kepatuhan tertinggi (95%), sedangkan TikTok memiliki tingkat kepatuhan yang relatif lebih rendah (75%) dibandingkan platform lainnya.



Sumber: Hasil Penelitian (2024)

Grafik 3 menunjukan investasi tahunan yang dikeluarkan oleh platform digital untuk keamanan cloud (dalam juta USD).(Suhada, 2023). Menampilkan investasi tahunan yang dikeluarkan oleh platform digital untuk keamanan data (dalam juta USD) (Hamad et al., 2023).

3.2 PEMBAHASAN

3.2.1 Efektivitas Praktik Keamanan

Hasil penelitian menunjukkan bahwa praktik keamanan utama seperti enkripsi data, manajemen akses berbasis peran, dan pemantauan real-time sangat efektif dalam menjaga keamanan data pengguna. Sebagai contoh, Netflix menggunakan AWS untuk melakukan enkripsi data streaming yang dapat menangkal lebih dari 95% ancaman siber selama periode puncak penggunaan. Selain itu, Google Cloud membantu Spotify mengelola data pengguna dengan cepat dan aman menggunakan BigQuery dan Dataflow.(Lad, 2024)

3.2.2 Tantangan dalam Implementasi

Meskipun praktik keamanan cukup efektif, tantangan seperti:

1. **Kepatuhan terhadap Regulasi**: TikTok menghadapi kesulitan dalam mematuhi regulasi berbeda di setiap negara, terutama di Amerika Serikat dan Eropa.
2. **Serangan Siber yang Terus Berkembang**: Penelitian dari Forrester (2023) menunjukkan bahwa metode serangan seperti ransomware dan phishing tetap menjadi ancaman bagi penyedia layanan cloud.(Kebande et al., 2021)

3.2.3 Solusi Inovatif untuk Mengatasi Tantangan

1. **Enkripsi Tingkat Lanjut**: Mengintegrasikan teknologi seperti Quantum Encryption untuk meningkatkan keamanan data.
2. **Kolaborasi Antara Platform Digital dan Penyedia Cloud**: Pemantauan bersama antara Netflix dan AWS telah membuktikan efektivitas dalam mengurangi insiden keamanan sebesar 30% dalam satu tahun.

3.2.4 Kontribusi Terhadap Transformasi Digital

Cloud computing berperan signifikan dalam mendukung transformasi digital. Namun, penelitian ini menekankan perlunya strategi adaptif untuk menghadapi ancaman yang terus berkembang, termasuk peningkatan investasi pada teknologi keamanan berbasis AI.

4. Kesimpulan

Penelitian ini membuktikan bahwa harapan yang disampaikan dalam pendahuluan, yaitu mengidentifikasi tantangan keamanan data dan strategi untuk mengatasinya dalam penerapan teknologi cloud computing pada platform digital, telah terpenuhi. Dari hasil dan diskusi, ditemukan bahwa enkripsi data, manajemen akses berbasis peran, dan pemantauan real-time adalah langkah strategis yang efektif dalam menjaga keamanan data. Namun, tantangan seperti kepatuhan terhadap regulasi yang kompleks dan ancaman serangan siber yang terus berkembang tetap memerlukan perhatian lebih lanjut.(Ali et al., 2015)

Selain itu, penelitian ini menegaskan pentingnya kolaborasi antara penyedia layanan cloud dan pengguna dalam mengelola risiko keamanan. Contohnya, kemitraan strategis antara Netflix dan AWS berhasil menurunkan insiden keamanan sebesar 30% dalam satu tahun.

Prospek Pengembangan dan Penerapan Penelitian

Berdasarkan hasil penelitian ini, beberapa prospek pengembangan dapat diusulkan:

1. **Inovasi Teknologi Keamanan:** Penelitian selanjutnya dapat mengeksplorasi penerapan enkripsi berbasis teknologi kuantum untuk meningkatkan keamanan data.
2. **Penggunaan AI dalam Keamanan:** Investasi pada teknologi berbasis kecerdasan buatan untuk mendeteksi dan merespons ancaman siber secara real-time.
3. **Model Kepatuhan Global:** Mengembangkan model kepatuhan universal yang dapat diadopsi oleh platform digital untuk mengatasi perbedaan regulasi antar negara.

Dari segi penerapan, strategi keamanan yang ditemukan dapat diadopsi oleh perusahaan lain yang menghadapi tantangan serupa, terutama yang bergantung pada teknologi cloud computing dalam operasi mereka. Ini berpotensi meningkatkan kepercayaan publik terhadap layanan digital di era transformasi digital yang semakin maju.(National Institute of Standards And Technology, 2018)

DAFTAR PUSTAKA

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*(February 2015), 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Engström, V., Johnson, P., Lagerström, R., Ringdahl, E., & Wällstedt, M. (2023). Automated Security Assessments of Amazon Web Services Environments. *ACM Transactions on Privacy and Security*, *26*(2). https://doi.org/10.1145/3570903

Hamad, D. J., Yalda, K. G., Tapus, N., & Okumus, I. T. (2023). A Survey on Security Issues in Cloud Systems. *Proceedings - RoEduNet IEEE International Conference*, *2023-Septe*. https://doi.org/10.1109/RoEduNet60162.2023.10274925

Iqra Naseer. (2023). AWS Cloud Computing Solutions: Optimizing Implementation for Businesses. *Statistics, Computing and Interdisciplinary Research*, *5*(2), 121–132. https://doi.org/10.52700/scir.v5i2.138

Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology (Singapore)*, *13*(1), 5–17. https://doi.org/10.1007/s41870-020-00585-8

Lad, S. (2024). Cybersecurity Trends: Integrating AI to Combat Emerging Threats in the Cloud Era. *Integrated Journal of Science and Technology*, *1*(8), 1–9.

National Institute of Standards And Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity 重要インフラのサイバーセキュリティを 改善するためのフレームワーク*.

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011). *Cloud Computing Security--Trends and Research Directions*. *July*, 524–531. https://doi.org/10.1109/services.2011.20

Suhada, M. I. P. N. (2023). Keamanan Dan Privasi Data Dalam Lingkungan CloudComputing: Tantangan Dan Solusi. *KOHESI : Jurnal Sains Dan Teknologi*, *Volume 01*(10), 71–80.

Sukhdeve, D. S. R., & Sukhdeve, S. S. (2023). Google Cloud Platform for Data Science. In *Google Cloud Platform for Data Science*. https://doi.org/10.1007/978-1-4842-9688-2