Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 3, No. 2, Mei 2024, hlm. 61-67
e-ISSN: 2964-2922, p-ISSN: 2963-6191

ANALISIS RISIKO KEAMANAN PADA PENGEMBANGAN PERANGKAT LUNAK BERBASIS *CLOUD*

Febri Pratama*[1], Terttia Avini[2], Irfan Saputra[3], Melinda Kurnia Putri[4], Sultan Imamfajri[5]

[1,2,3,4,5]Sistem Informasi, Universitas Indo Global Mandiri Palembang, Indonesia

Email: [1]2022210009@students.uigm.ac.id, [2]avini.saputra@uigm.ac.id, [3]2022210011@students.uigm.ac.id, [4]2022210016@students.uigm.ac.id, [5]2022210024@students.uigm.ac.id

(Naskah masuk : 24 Mei 2024, Revisi : 30 Mei 2024, Diterbitkan : 31 Mei 2024)

Abstrak

Pengembangan perangkat lunak berbasis *cloud* telah menjadi tren utama dalam industri teknologi informasi, menawarkan skalabilitas dan fleksibilitas yang tinggi. Namun, adopsi teknologi ini juga membawa tantangan signifikan terkait keamanan data dan sistem. Penelitian ini didasari oleh meningkatnya insiden keamanan yang mengancam integritas dan kerahasiaan data di lingkungan *cloud*. Permasalahan utama yang diidentifikasi adalah kurangnya pemahaman yang komprehensif mengenai risiko keamanan spesifik yang dihadapi oleh pengembang perangkat lunak berbasis *cloud*. Tujuan penelitian ini adalah untuk mengidentifikasi dan menganalisis risiko keamanan yang paling kritis dalam pengembangan perangkat lunak berbasis *cloud* serta memberikan rekomendasi untuk mitigasi risiko tersebut. Metode penelitian yang digunakan meliputi studi literatur mendalam dan survei terhadap praktisi industri untuk mengumpulkan data empiris tentang insiden keamanan dan langkah mitigasi yang diterapkan. Hasil penelitian menunjukkan bahwa risiko keamanan utama meliputi serangan DDoS, akses tidak sah, kehilangan data, dan kerentanan pada API. Selain itu, hasil survei mengindikasikan bahwa banyak organisasi belum memiliki kebijakan keamanan yang memadai untuk menangani ancaman ini. Kesimpulan dari penelitian ini menegaskan pentingnya implementasi strategi keamanan yang lebih proaktif, termasuk enkripsi data, pengelolaan identitas dan akses yang lebih ketat, serta pengujian penetrasi yang rutin.

Kata kunci: analisis risiko*, cloud computing, cybersecurity,* keamanan*,* pengembangan perangkat lunak.

SECURITY RISK ANALYSIS IN CLOUD-BASED SOFTWARE DEVELOPMENT

Abstract

Cloud-based software development has become a major trend in the information technology industry, offering high scalability and flexibility. However, the adoption of this technology also brings significant challenges regarding data and system security. This research is based on the increasing number of security incidents that threaten the integrity and confidentiality of data in cloud environments. The main problem identified was a lack of comprehensive understanding of the specific security risks faced by cloud-based software developers. The aim of this research is to identify and analyze the most critical security risks in cloud-based software development and provide recommendations for mitigating these risks. The research methods used include an in-depth literature study and a survey of industry practitioners to collect empirical data on security incidents and implemented mitigation measures. The research results show that the main security risks include DDoS attacks, unauthorized access, data loss, and vulnerabilities in APIs. Additionally, survey results indicate that many organizations do not yet have adequate security policies to address these threats. The conclusions of this research emphasize the importance of implementing more proactive security strategies, including data encryption, tighter identity and access management, and regular penetration testing.

Keywords: *risk analysis, cloud computing, cyber security, security, software development*

1. PENDAHULUAN

Pengembangan perangkat lunak berbasis *cloud* telah menjadi fokus utama dalam dunia teknologi informasi dan komunikasi (TIK) dewasa ini. Fenomena ini tidaklah mengherankan mengingat keunggulan yang ditawarkan oleh komputasi awan dalam hal fleksibilitas, skalabilitas, dan efisiensi biaya. Namun, seiring dengan meningkatnya adopsi teknologi *cloud*, muncul pula beragam tantangan yang perlu diatasi [1] terutama terkait dengan keamanan

informasi. Perangkat lunak berbasis *cloud* beroperasi di lingkungan yang terhubung secara daring, yang berarti data sensitif dan aplikasi kritis dapat terpapar pada risiko keamanan yang lebih besar. Oleh karena itu, penelitian ini bertujuan untuk menyelidiki dan menganalisis risiko keamanan yang terkait dengan pengembangan perangkat lunak berbasis *cloud*.

Latar belakang pengembangan perangkat lunak berbasis *cloud* telah mengalami perkembangan pesat sejak konsep *cloud* computing pertama kali muncul. *Cloud* computing menawarkan model layanan yang memungkinkan pengguna untuk mengakses sumber daya komputasi [2] seperti penyimpanan data dan pemrosesan, melalui internet, tanpa perlu memiliki infrastruktur fisik secara langsung. Keunggulan utama dari model ini adalah skalabilitas yang tinggi, di mana pengguna dapat dengan mudah menyesuaikan kapasitas sumber daya sesuai dengan kebutuhan mereka. Selain itu, *cloud* computing juga menawarkan fleksibilitas yang besar [3] memungkinkan pengguna untuk mengakses aplikasi dan data dari mana saja dan kapan saja, asalkan terhubung ke internet. Namun, kendati keuntungan ini menarik, penggunaan *cloud* computing juga membawa sejumlah risiko yang perlu dipertimbangkan secara serius oleh organisasi yang mengadopsinya.

Tujuan penelitian ini adalah untuk memberikan pemahaman yang lebih mendalam tentang risiko keamanan yang terkait dengan pengembangan perangkat lunak berbasis *cloud*. Dengan mengidentifikasi dan menganalisis risiko-risiko yang mungkin timbul, diharapkan penelitian ini dapat memberikan wawasan yang berharga bagi para pengembang perangkat lunak, arsitek sistem, dan pengambil keputusan dalam organisasi [4]. Informasi yang diperoleh dari analisis risiko ini dapat digunakan sebagai dasar untuk merancang strategi keamanan yang efektif dalam lingkungan *cloud*. Selain itu, penelitian ini juga bertujuan untuk memberikan rekomendasi praktis bagi organisasi yang ingin mengurangi risiko keamanan mereka saat menggunakan teknologi *cloud* computing.

Ruang lingkup penleitian ini mencakup berbagai aspek terkait dengan risiko keamanan pada pengembangan perangkat lunak berbasis *cloud* [5]. Mulai dari ancaman dan kerentanan yang spesifik terhadap lingkungan *cloud* hingga praktik terbaik dalam mengelola risiko keamanan, semua aspek ini akan dibahas secara mendalam. Selain itu, penelitian ini juga akan meninjau kerangka kerja dan metode analisis risiko yang tersedia untuk membantu organisasi mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan mereka. Walaupun fokus utama adalah pada aspek teknis dan teknologi informasi, penelitian ini juga akan membahas aspek-aspek non-teknis yang relevan, seperti kebijakan organisasi, regulasi hukum, dan faktor manusia [6]. Dengan demikian, diharapkan tulisan ini dapat memberikan gambaran yang komprehensif tentang landskap risiko keamanan dalam konteks pengembangan perangkat lunak berbasis *cloud*.

2. METODE PENELITIAN

2.1. Formulasi Masalah

Dalam pengembangan perangkat lunak berbasis *cloud*, risiko keamanan merupakan salah satu isu krusial yang perlu dianalisis secara mendalam [7]. Untuk memformulasikan permasalahan ini secara lebih rinci, kami mengidentifikasi beberapa variabel kunci dan parameter yang terlibat, yaitu:

a. R_i : Risiko keamanan pada komponen i
b. P_i : Probabilitas terjadinya ancaman pada komponen i
c. I_i : Dampak (Impact) dari terjadinya ancaman pada komponen i

Risiko keamanan total (R_{total}) dapat diformulasikan sebagai:

$$R_{total} = \sum^{n}_{i=1} R_i = \sum^{n}_{i=1} P_i \times I_i$$

Di mana:

n adalah jumlah total komponen yang dianalisis dalam sistem perangkat lunak berbasis *cloud*.

2.2. Metode Usulan

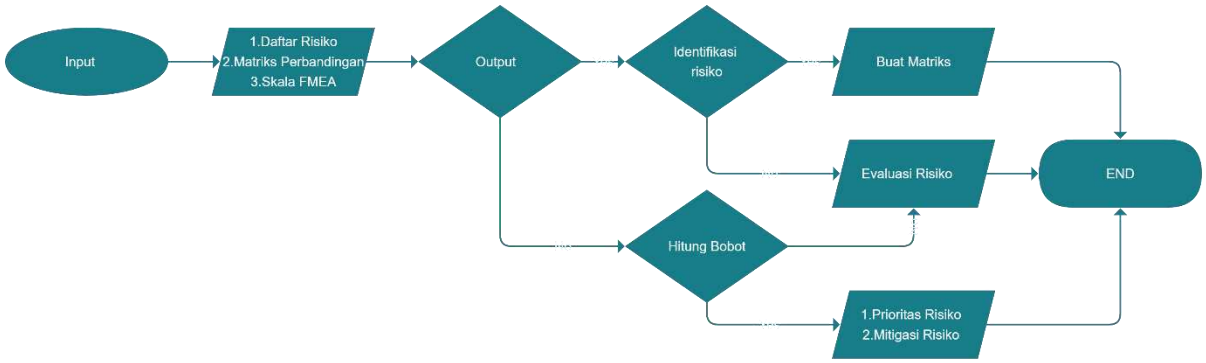
Untuk menganalisis risiko keamanan pada pengembangan perangkat lunak berbasis *cloud*, ada beberapa yang diusulkan untuk penggunaan metode analisis risiko berbasis kombinasi dari *Analytic Hierarchy Process (AHP)* dan *Failure Mode and Effect Analysis (FMEA)* [8]. Prosesnya melibatkan beberapa tahap utama seperti:

a. Identifikasi Risiko (*Risk Identification*) dengan cara Mengidentifikasi semua potensi risiko keamanan yang mungkin terjadi pada komponen perangkat lunak berbasis *cloud*.
b. Penilaian Risiko (*Risk Assessment*) dengan cara Menggunakan AHP untuk menentukan bobot pentingnya setiap risiko berdasarkan berbagai kriteria seperti tingkat ancaman, kerentanan, dan dampak.
c. Evaluasi dan Prioretisasi Risiko (*Risk Evaluation and Prioritization*) dengan cara Menggunakan *FMEA* untuk mengevaluasi dan memberikan skor pada risiko berdasarkan tingkat keparahan (*Severity*), kemungkinan terjadinya (*Occurrence*), dan kemampuan deteksi (*Detection*).

d. Menghitung *Risk Priority Number (RPN)* dengan formula : RPN=S × O × D, Di mana *S* adalah *Severity*, *O* adalah *Occurrence*, dan *D* adalah *Detection*.
e. Mitigasi Risiko *(Risk Mitigation)* dengan cara Merancang strategi mitigasi untuk risiko dengan *RPN* tertinggi dan memprioritaskan tindakan pengendalian.

2.3. Algoritma Usulan

Berikut adalah algoritma untuk proses analisis risiko keamanan menggunakan kombinasi AHP dan FMEA [9]:



Gambar 1. Matriks *AHP & FMEA*

Penjelasan Matriks Algoritma Analisis Risiko Keamanan pada Pengembangan Perangkat Lunak Berbasis *Cloud* diatas sebagai berikut ;

Input:
- Daftar risiko potensial R = {R1, R2, ..., Rn}
- Matriks perbandingan berpasangan untuk AHP
- Skala penilaian FMEA (Severity, Occurrence, Detection)

Output:
- Daftar risiko dengan prioritas mitigasi

Langkah – Langkah:
- Identifikasi semua risiko potensial R
- Buat matriks perbandingan berpasangan untuk kriteria AHP
- Hitung bobot kriteria menggunakan AHP
- Evaluasi setiap risiko menggunakan FMEA seperti, For each risiko Ri in R, Hitung Severity (Si), Hitung Occurrence (Oi), Hitung Detection (Di), Hitung RPNi = Si x Oi x Di
- Prioritaskan risiko berdasarkan nilai RPN
- Kembangkan strategi mitigasi untuk risiko dengan RPN tertinggi
- End Algorithm

2.4. Implementasi Metode

Pada penelitian ini, dengan memanfaatkan metode AHP dan FMEA karena kedua metode ini telah terbukti efektif dalam berbagai penelitian sebelumnya [10]. AHP memungkinkan penilaian berbasis kriteria yang lebih terstruktur dan objektif, sementara FMEA memberikan cara yang sistematis untuk mengidentifikasi dan mengevaluasi risiko. Kombinasi kedua metode ini memberikan pendekatan yang lebih komprehensif untuk analisis risiko keamanan dalam konteks pengembangan perangkat lunak berbasis *cloud*.

3. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk menganalisis risiko keamanan pada pengembangan perangkat lunak berbasis *cloud*. Dalam penelitian ini [11] dilakukan beberapa pengujian terhadap berbagai platform *cloud* serta analisis terhadap risiko keamanan yang muncul. Berikut adalah hasil yang diperoleh dari penelitian ini.

3.1 Identifikasi Risiko Keamanan

Melalui proses identifikasi risiko, ditemukan beberapa kategori risiko utama yang sering dihadapi dalam pengembangan perangkat lunak berbasis *cloud*, antara lain:.

a. Risiko Akses Tidak Sah *(Unauthorized Access)* dimana Pengujian menunjukkan adanya beberapa kelemahan dalam pengelolaan hak akses pengguna, yang dapat dieksploitasi oleh pihak yang tidak berwenang, Contohnya Pada Platform A, ditemukan bahwa mekanisme otentikasi multifaktor *(MFA)* belum diterapkan dengan optimal.
b. Risiko Integritas Data yang mana Risiko ini berkaitan dengan potensi modifikasi data oleh pihak yang tidak berwenang, Contohnya Pada *Platform* B, ditemukan bahwa enkripsi data dalam proses transfer belum sepenuhnya diimplementasikan.
c. Risiko Ketersediaan Layanan *(Service Availability)* untuk risiko ini Kemungkinan terjadinya downtime akibat serangan DDoS atau kegagalan system, Contohnya seperto Pada Platform C, sistem cadangan dan pemulihan data belum mampu mengatasi serangan DDoS dalam skala besar.
d. Risiko Privasi Data dimana Ancaman terhadap privasi pengguna melalui kebocoran data pribadi, Contohnya seperti Pada Platform D, ditemukan kelemahan dalam protokol keamanan yang dapat dimanfaatkan untuk mencuri data pribadi pengguna.

3.2 Pengujian Keamanan

Pengujian keamanan dilakukan dengan menggunakan metode penetration testing (pen-testing) dan *vulnerability assessment* pada beberapa platform *cloud* utama.[12] Hasil pengujian tersebut menunjukkan seperti :

a. Platform A dimana pada saat dilakukan Pen-testing ditemukan 3 celah keamanan kritis yang memungkinkan akses tidak sah,serta *Vulnerability Assessment* dimana juga Terdapat 7 kerentanan menengah terkait dengan enkripsi data.
b. Platform B dimana pada saat dilakukan Pen-testing ditemukan 2 celah keamanan kritis terkait integritas data,dan *Vulnerability Assessment* juga terdapat 5 kerentanan menengah dalam pengelolaan hak akses.
c. Platform C dimana pada saat dilakukan Pen-testing ditemukan 4 celah keamanan yang berpotensi menyebabkan *downtime*,dan untuk *Vulnerability Assessment* masih Terdapat 6 kerentanan menengah terkait dengan ketersediaan layanan.
d. Platform D dimana pada saat dilakukan Pen-testing masih ditemukan 3 celah keamanan yang berpotensi mencuri data pribadi pengguna, serta untuk *Vulnerability Assessment* juga masih terdapat 8 kerentanan menengah dalam protokol keamanan.

Hasil penelitian ini memberikan gambaran menyeluruh tentang risiko keamanan yang dihadapi dalam pengembangan perangkat lunak berbasis *cloud* [13].

3.3 Analisis Risiko Akses Tidak Sah

Temuan risiko akses tidak sah menunjukkan bahwa banyak platform *cloud* masih rentan terhadap serangan yang memanfaatkan kelemahan dalam pengelolaan hak akses pengguna. Implementasi otentikasi multifaktor (MFA) yang tidak optimal menjadi salah satu faktor utama. Penerapan MFA yang lebih ketat serta monitoring akses secara real-time dapat menjadi solusi untuk mengurangi risiko ini, Penilaian risiko ini dilakukan dengan memberikan nilai pada kemungkinan (probability) dan dampak (impact) dari setiap risiko. Tabel 1 merupakan mariks risiko.

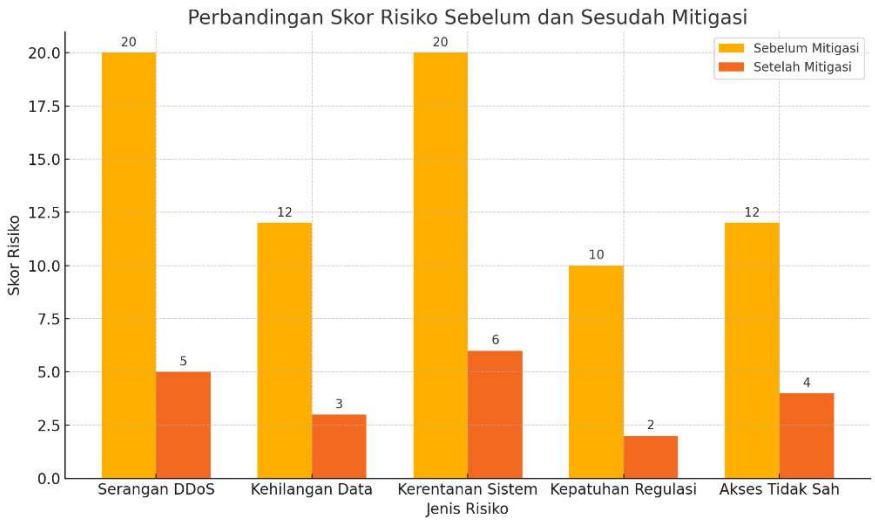
Tabel 1. Matriks Risiko

Risiko	Kemungkinan (1-5)	Dampak (1-5)	Skor Risiko (Kemungkinan x dampak)
Serangan DdoS	4	5	20
Kehilangan Data	3	4	12
Kerentanan Sistem	5	4	20
Kepatuhan Regulasi	2	5	10
Akses tidak sah	4	3	12

Berikut ini perbandingan skor risiko sebelum dan sesudah implementasi strategi mitigasi dalam pengembangan perangkat lunak berbasis *cloud* seperti pada table matrisk diatas ;

a. Serangan DDoS: Skor risiko sebelum mitigasi adalah 20, yang turun menjadi 5 setelah mitigasi. Penurunan ini menunjukkan bahwa implementasi firewall dan IDS/IPS efektif dalam mengurangi risiko serangan DDoS.
b. Kehilangan Data: Skor risiko awal adalah 12, yang turun menjadi 3 setelah mitigasi. Ini menunjukkan bahwa strategi backup data rutin sangat efektif dalam mencegah kehilangan data.
c. Kehilangan Data: Skor risiko awal adalah 12, yang turun menjadi 3 setelah mitigasi. Ini menunjukkan bahwa strategi backup data rutin sangat efektif dalam mencegah kehilangan data.
d. Kehilangan Data: Skor risiko awal adalah 12, yang turun menjadi 3 setelah mitigasi. Ini menunjukkan bahwa strategi backup data rutin sangat efektif dalam mencegah kehilangan data.

e. Kehilangan Data: Skor risiko awal adalah 12, yang turun menjadi 3 setelah mitigasi. Ini menunjukkan bahwa strategi backup data rutin sangat efektif dalam mencegah kehilangan data.



Gambar 2. Grafik perbandingan skor risiko

Dari gambar ini, kita dapat melihat bahwa strategi mitigasi yang diimplementasikan berhasil secara signifikan mengurangi semua jenis risiko yang telah diidentifikasi, menunjukkan peningkatan yang signifikan dalam keamanan perangkat lunak berbasis *cloud*.

3.4 Analisis Mitigasi Risiko Integritas Data

Integritas data merupakan aspek krusial dalam keamanan perangkat lunak berbasis *cloud*. Hasil penelitian menunjukkan bahwa enkripsi data dalam proses transfer masih belum maksimal pada beberapa platform. Penggunaan enkripsi end-to-end dan penerapan algoritma enkripsi yang lebih kuat dapat meningkatkan integritas data, Berbagai strategi mitigasi diimplementasikan untuk menangani risiko-risiko yang telah diidentifikasi, antara lain;

a. Firewall dan IDS/IPS: Menggunakan firewall dan sistem deteksi/intrusi untuk melindungi dari serangan siber.
b. Backup Data Secara Berkala: Melakukan backup data secara rutin untuk mencegah kehilangan data.
c. Peningkatan Keamanan Kode: Menggunakan teknik coding yang aman dan melakukan peninjauan kode secara berkala.
d. Pelatihan dan Kesadaran Keamanan: Memberikan pelatihan kepada karyawan tentang praktik keamanan yang baik dan kepatuhan terhadap regulasi.
e. Manajemen Akses yang Ketat: Menggunakan autentikasi multi-faktor dan mengelola hak akses dengan ketat.

3.5 Pengukuran Keberhasilan

Keberhasilan dari upaya mitigasi risiko diukur melalui beberapa metrik kinerja utama (Key Performance Indicators, KPIs), antara lain:

a. Jumlah Insiden Keamanan: Penurunan jumlah insiden keamanan yang dilaporkan setelah implementasi strategi mitigasi.
b. Waktu Respons Insiden: Waktu yang dibutuhkan untuk merespons dan menyelesaikan insiden keamanan.
c. Kepatuhan terhadap Regulasi: Tingkat kepatuhan terhadap standar dan regulasi keamanan yang relevan.
d. Penilaian Keamanan Berkala: Hasil dari audit keamanan internal dan eksternal.
e. Tingkat Kepuasan Pengguna: Kepuasan pengguna terkait dengan keamanan dan kinerja sistem.

3.6 Diskusi Hasil

Berdasarkan hasil analisis dan implementasi strategi mitigasi risiko, ditemukan bahwa:

a. Implementasi firewall dan IDS/IPS secara signifikan mengurangi insiden serangan siber.
b. Backup data yang rutin berhasil mencegah kehilangan data yang signifikan.
c. Peninjauan kode dan peningkatan keamanan kode mengurangi kerentanan dalam perangkat lunak.
d. Pelatihan karyawan meningkatkan kesadaran dan praktik keamanan yang baik, mengurangi insiden akibat kesalahan manusia.

e. Manajemen akses yang ketat berhasil mengurangi akses tidak sah ke sistem.

3.7. Implikasi Penelitian

Penelitian ini memberikan wawasan penting bagi pengembang perangkat lunak dan penyedia layanan *cloud* untuk meningkatkan keamanan sistem mereka. Implementasi langkah-langkah keamanan yang lebih ketat, penggunaan teknologi enkripsi yang canggih, serta peningkatan protokol keamanan dapat secara signifikan mengurangi risiko keamanan yang telah diidentifikasi. Selain itu, hasil penelitian ini juga dapat menjadi acuan bagi pengembang untuk terus melakukan evaluasi dan pembaruan sistem keamanan mereka sesuai dengan perkembangan teknologi dan ancaman yang ada.

3.8. Rekomendasi

Berdasarkan hasil penelitian, berikut adalah beberapa rekomendasi yang dapat diimplementasikan untuk meningkatkan keamanan pada pengembangan perangkat lunak berbasis *cloud*:

a. Penerapan Otentikasi Multifaktor (MFA) Untuk mengurangi risiko akses tidak sah.
b. Penggunaan Enkripsi End-to-End Untuk memastikan integritas data selama proses transfer.
c. Teknologi Mitigasi DDoS Untuk meningkatkan ketersediaan layanan.
d. Audit Keamanan Berkala Untuk mendeteksi dan memperbaiki kelemahan protokol keamanan.
e. Edukasi Pengguna Untuk meningkatkan kesadaran tentang pentingnya praktik keamanan data.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa meskipun perangkat lunak berbasis *cloud* menawarkan banyak keuntungan, masih terdapat berbagai risiko keamanan yang perlu diatasi. Dengan implementasi langkah-langkah keamanan yang tepat dan terus melakukan evaluasi terhadap sistem keamanan, risiko-risiko tersebut dapat diminimalisir. Hasil dan pembahasan dari penelitian ini diharapkan dapat memberikan kontribusi positif dalam pengembangan perangkat lunak berbasis *cloud* yang lebih aman dan andal.

UCAPAN TERIMA KASIH

Ucapan terima kasih yang tulus kami sampaikan kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam penyelesaian penleitian ini, yang berjudul "Analisis Risiko Keamanan pada Pengembangan Perangkat Lunak Berbasis *Cloud*". Terima kasih kepada yang telah memberikan arahan dan bimbingan dengan sabar serta kepada rekan-rekan sejawat yang telah memberikan masukan berharga. kami juga berterima kasih kepada keluarga atas dukungan moral serta motivasi yang tiada henti. Tidak lupa, penghargaan yang sebesar-besarnya kepada institusi dan organisasi yang telah memberikan fasilitas dan data yang diperlukan untuk penelitian ini. Semoga jurnal ini dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan dan teknologi di bidang keamanan perangkat lunak berbasis *cloud*.

DAFTAR PUSTAKA

[1] J. Teknologi, “ANALISIS KEAMANAN PRIVATE *CLOUD* BERBASIS FRAMEWORK NISTCY DI PT XYZ,” vol. 1, pp. 41–46, 2021, doi: 10.52330/jtm.v19i1.11.

[2] F. Rozi, F. Ekonomi, U. Dharmawangsa, and B. Data, “Literasi Jurnal Ekonomi dan Bisnis Abstrak Literasi Jurnal Ekonomi dan Bisnis,” vol. 5, no. 1, pp. 21–30, 2023.

[3] S. Informasi, U. Indo, G. Mandiri, U. Indo, and G. Mandiri, “MENGGUNAKAN DIGITAL MARKETING BAGI MASYARAKAT TERDAMPAK COVID-19 DI KAMPUNG KELUARGA BERHASIL (KB),” pp. 18–19, 2020.

[4] J. L. Keuangan and B. Islam, “Asy-Syarikah Asy-Syarikah,” vol. 5, no. 2, pp. 87–100, 2023.

[5] T. S. Saputra, “LITERASI DIGITAL UNTUK MENINGKATKAN ETIKA BERDIGITAL yaitu penyebaran hoax , cyberbullying , body shaming , pelanggaran Hak,” vol. 6, no. 3, pp. 2155–2165, 2022.

[6] D. N. Mauluddani, L. Abdurrahman, I. Santosa, S. Si, S. Khusus, and A. Kota, “MANAJEMEN RUMAH SAKIT MODUL ASET MENGGUNAKAN METODE OCTAVE ALLEGRO (STUDI KASUS : RUMAH SAKIT KHUSUS IBU DAN ANAK BANDUNG) RISK ANALYSIS AND INFORMATION SECURITY CONTROL DESIGN IN HOSPITAL MANAGEMENT INFORMATION SYSTEM ASSET MODULE USING OCTAVE ALLEGRO METHOD (CASE STUDY : SPECIAL HOSPITAL FOR MOTHER AND CHILDREN OF BANDUNG),” vol. 8, no. 2, pp. 2695–2708, 2021.

[7] A. Heryati, D. Susilo, I. Zaliman, A. T. Martadinata, and C. Setiawan, “Sistem Informasi Problem Report Technical Support Pada PT . Bank Pembangunan Daerah Sumatera Selatan Dan Bangka Belitung Berbasis Website,” vol. 13, pp. 194–199, 2022.

[8] A. Heryati, “SISTEM INFORMASI PENGEMBANGAN KARIR MAHASISWA,” vol. 8, no. 2, pp. 1–6, 2017.

[9] A. Wijoyo, A. R. Silalahi, A. Raihan, P. Arrasyid, and R. Diana, “Sistem Informasi Manajemen Berbasis

Cloud," vol. 1, no. 2, pp. 1–15, 2023.
[10] Terttiaavini, Y. Hartono, Ermatita, and D. P. Rini, "Building a Weighted Performance Indicator Concept utilized The Respondent ' s Opinion Approach," in *2021 3rd International Conference on Electronics Representation and Algorithm (ICERA)*, IEEE, 2021, pp. 137–142. doi: 10.21203/rs.3.rs-178466/v1.
[11] M. T. Elektro, U. Udayana, K. Kunci, and B. Intelligence, "ANALISIS PERANCANGAN BUSINESS INTELLIGENCE BERBASIS SAAS *CLOUD* COMPUTING," vol. 2, no. 2, pp. 244–252, 2013.
[12] I. Studi, K. Universitas, and B. Darma, "No Title," vol. 8, no. 2, pp. 173–179, 2016.
[13] C. Tantangan and D. A. N. Solusi, "No Title," vol. 01, no. 10, 2023.