Terbit online pada laman web jurnal: **https://jurnal.plb.ac.id/index.php/tematik/index**

T E M A T I K

Jurnal **Teknologi Informasi Komunikasi (e-Journal)**

Vol. 12 No. 1 (2025) 94 - 100 ISSN Media Elektronik: 2443-3640

Arsitektur Keamanan Komputasi Awan Berbasis Multi-Layer di Internet Nirkabel dengan Pendekatan SeaaS

Multi-Layer Cloud Computing Security Architecture in Wireless Internet with SeaaS Approach

Zen Munawar[1], Sri Sutjiningtyas[2], Novianti Indah Putri[3], Milla Marlina[4], Rita Komalasari[5], Herru Soerjono[6]
[1,5]Manajemen Informatika, Politeknik LP3I,
[2]Teknik Informatika, Ilmu Komputer dan Informatika, Universitas Nurtanio
[3]Sistem Informasi, Ilmu Komputer dan Sistem Informasi, Universitas Kebangsaan Republik Indonesia
[4,6]Administrasi Bisnis, Politeknik LP3I,
[1]munawarzen@gmail.com, [2]srisutjiningtyas70@gmail.com, [3]noviantiindahputri2021@gmail.com, [4]millamarlina@pln.ac.id, [5]ritakomalasari@plb.ac.id, [6]herrusoerjono2022@gmail.com.

Abstract

This research aims to propose an effective cloud computing security architecture in the context of wireless internet. With the increasing use of cloud computing services, the security challenges faced are becoming increasingly complex, especially related to data privacy and cyber threats. To address these issues, we apply a multi-layer approach and Security as a Service (SeaaS) in designing an adaptive and secure architecture. The method used involves simulation and system testing of the proposed architecture. We implement the architecture in a controlled environment to observe the performance and security response, and conduct tests on various attack scenarios to evaluate its effectiveness. The results of the study show that this architecture is able to overcome various security risks faced by cloud computing service users in a wireless environment. The discussion analyzes the results obtained from the architecture testing. The advantage of this architecture is its ability to adapt to various types of attacks through a multi-layer approach, which improves the overall level of security. However, there are also disadvantages in terms of implementation complexity that may require more resources for its management. The conclusion of this study confirms that the proposed cloud computing security architecture makes a significant contribution to improving the security of services in wireless internet, while offering the flexibility and adaptability needed to meet the needs of diverse users.

Keywords: Wireless Internet; cloud computing; security architecture

Abstrak

Penelitian ini bertujuan untuk mengusulkan arsitektur keamanan komputasi awan yang efektif dalam konteks internet nirkabel. Dengan meningkatnya penggunaan layanan komputasi awan, tantangan keamanan yang dihadapi menjadi semakin kompleks, terutama terkait dengan privasi data dan ancaman siber. Untuk mengatasi masalah ini, kami menerapkan pendekatan multi-layer dan Security as a Service (SeaaS) dalam merancang arsitektur yang adaptif dan aman. Metode yang digunakan melibatkan simulasi dan pengujian sistem pada arsitektur yang diusulkan. Kami mengimplementasikan arsitektur di lingkungan yang terkendali untuk mengamati performa dan respons keamanan, serta melakukan pengujian terhadap berbagai skenario serangan untuk mengevaluasi efektivitasnya. Hasil penelitian menunjukkan bahwa arsitektur ini mampu mengatasi berbagai risiko keamanan yang dihadapi oleh pengguna layanan komputasi awan di lingkungan nirkabel. Pembahasan menganalisis hasil yang diperoleh dari pengujian arsitektur. Kelebihan dari arsitektur ini adalah kemampuannya untuk menyesuaikan diri dengan berbagai jenis serangan melalui pendekatan multi-layer, yang meningkatkan tingkat keamanan secara keseluruhan. Namun, terdapat juga kekurangan dalam hal kompleksitas implementasi yang mungkin memerlukan sumber daya lebih untuk pengelolaannya. Kesimpulan penelitian ini menegaskan bahwa arsitektur keamanan komputasi awan yang diusulkan memberikan kontribusi signifikan terhadap peningkatan keamanan layanan di internet nirkabel, serta menawarkan fleksibilitas dan adaptabilitas yang diperlukan untuk memenuhi kebutuhan pengguna yang beragam.

Kata kunci: Internet nirkabel; komputasi awan; arsitektur keamanan

1. Pendahuluan

Dalam komputasi awan, data dan aplikasi berada pada server web di awan . Ketika berbicara tentang sistem komputasi awan, terbagi menjadi dua bagian: front end

Diterima Redaksi: 1-06-2025 | Selesai Revisi: 28-06-2025 | Diterbitkan Online: 28-06-2025

dan back end [1]. Front end adalah sisi yang dilihat oleh pengguna komputer, atau klien. Back end sistem adalah berbagai komputer, server, dan sistem penyimpanan data yang menciptakan layanan komputasi awan. Semuanya terhubung satu sama lain melalui jaringan, biasanya internet. Semua sistem komputasi awan tidak memiliki antarmuka pengguna yang sama [2]. Karena prospek bisnis komputasi awan yang luar biasa, banyak perusahaan yang terkait dengan internet nirkabel telah menyediakan berbagai layanan komputasi awan. Memperkenalkan komputasi awan ke internet nirkabel menyebabkan perubahan arsitektur internet nirkabel, dan menimbulkan banyak masalah keamanan baru seperti keamanan data lintas domain dan perlindungan privasi, keamanan lingkungan virtual yang berjalan, dan monitor keamanan lintas domain. Untuk menghadapi tantangan ini, perlu untuk meneliti risiko keamanan terkait dan merancang arsitektur komputasi awan yang aman untuk meletakkan dasar bagi keberhasilan penerapannya di internet nirkabel [3].

Perlindungan data merupakan isu penting dalam lingkungan komputasi awan. Terdapat beberapa karakteristik yang menjadikan komputasi awan sebagai salah satu sektor dengan tingkat pertumbuhan tercepat dalam ekonomi modern [4]. Awan tidak memiliki batas dan data dapat secara fisik berada di mana saja di dunia. Jadi fenomena ini menimbulkan isu serius terkait autentikasi pengguna dan kerahasiaan data [5]. Oleh karena itu, diusulkan Arsitektur keamanan komputasi awan di internet nirkabel yang melakukan autentikasi, verifikasi, dan transfer data terenkripsi, sehingga menjaga kerahasiaan data [6]. Dengan menganalisis risiko keamanan teknologi komputasi awan dan arsitektur aman yang tersedia, maka perlu merancang arsitektur komputasi awan umum yang aman dengan antarmuka pengguna yang multi-hierarki, multi-level, elastisitas, lintas platform, dan terpadu di internet nirkabel sesuai dengan prinsip SeaaS (Security as a Service) dan karakteristik internal internet nirkabel, yaitu beberapa mode akses, berbagai operasi perusahaan, dan persyaratan keamanan pengguna yang berbeda, dan lain-lain.

Meskipun banyak solusi keamanan yang telah dikembangkan, masih terdapat kekurangan dalam hal adaptabilitas dan fleksibilitas terhadap berbagai jenis serangan yang muncul di lingkungan nirkabel. Penelitian ini berkontribusi dengan mengusulkan arsitektur yang tidak hanya aman tetapi juga dapat disesuaikan dengan kebutuhan spesifik pengguna, sehingga mengisi gap yang ada dalam penelitian sebelumnya.

2. Metode Penelitian

2.1. Pendekatan dan Pengumpulan Data Penelitian

Pendekatan penelitian ini menggunakan metode kualitatif dan kuantitatif. Metode kualitatif digunakan untuk memahami fenomena keamanan dalam komputasi awan dan internet nirkabel, sedangkan metode kuantitatif digunakan untuk mengukur tingkat keamanan dan efektivitas arsitektur yang diusulkan. Data yang dikumpulkan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer meliputi hasil wawancara dengan ahli keamanan siber, survei pengguna tentang pengalaman mereka dalam menggunakan layanan komputasi awan, dan data eksperimen terkait implementasi arsitektur keamanan. Sedangkan data sekunder meliputi literatur terkait keamanan komputasi awan, laporan penelitian sebelumnya, dan dokumen kebijakan yang relevan.

Data yang dikumpulkan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer meliputi hasil wawancara dengan ahli keamanan siber, survei pengguna tentang pengalaman mereka dalam menggunakan layanan komputasi awan, dan data eksperimen terkait implementasi arsitektur keamanan. Sedangkan data sekunder meliputi literatur terkait keamanan komputasi awan, laporan penelitian sebelumnya, dan dokumen kebijakan yang relevan.

Teknik analisis data, data yang dikumpulkan akan dianalisis dengan menggunakan analisis kualitatif yaitu data wawancara dan survei akan dianalisis menggunakan pendekatan tematik untuk mengidentifikasi pola dan tema yang muncul. Sedangkan analisis kuantitatif, data survei akan dianalisis menggunakan statistik deskriptif untuk menggambarkan karakteristik responden dan tingkat keamanan yang dirasakan. Validitas data akan dijaga melalui triangulasi, menggunakan berbagai sumber data (wawancara, survei, dan studi literatur) untuk memverifikasi temuan. Uji coba dengan melakukan uji coba awal terhadap kuesioner untuk memastikan bahwa pertanyaan yang diajukan dapat dipahami dengan baik oleh responden.

Subjek dan objek penelitian, subjek penelitian yaitu para ahli keamanan siber, pengguna layanan komputasi awan, dan penyedia layanan komputasi awan. Objek penelitian adalah arsitektur keamanan komputasi awan yang diusulkan dan implementasinya dalam lingkungan internet nirkabel. Penelitian ini dilakukan selama enam bulan, mulai dari November 2024 hingga April 2025, dengan tahapan pengumpulan data, analisis, dan penyusunan laporan. Sumber data yang digunakan dalam penelitian ini terdiri dari dokumen resmi, kebijakan keamanan dari penyedia layanan komputasi awan. Literatur akademik berupa jurnal dan artikel yang membahas keamanan dalam komputasi awan. Data survei yaitu hasil kuesioner yang disebarkan kepada pengguna.

DOI: https://doi.org/10.38204/tematik
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Eksperimen dilakukan melalui simulasi dan pengujian sistem pada arsitektur yang diusulkan. Penelitian mengimplementasikan arsitektur di lingkungan yang dikontrol untuk mengamati performa dan respons keamanan, serta melakukan pengujian terhadap berbagai skenario serangan untuk mengevaluasi efektivitasnya.

2.2. Karakteristik Komputasi Awan

Pada bulan Januari 2011, Institut Standar dan Teknologi Nasional AS menjelaskan dengan jelas dalam definisi komputasi awan (draft) bahwa karakteristik esensialnya mencakup akses jaringan yang luas melalui berbagai platform, yaitu telepon nirkabel, laptop, PDA, dan desktop tradisional lainnya [7]. Artinya, internet nirkabel dapat ditanamkan ke dalam arsitektur teknologi komputasi awan. Setelah menerapkan teknologi komputasi awan, internet nirkabel menghadapi serangkaian masalah keamanan baru karena karakteristik intrinsik teknologi komputasi awan (misalnya, virtualisasi, multitenant, dinamis, terbuka, dan rumit, dan lain-lain). Dalam beberapa tahun terakhir, menganalisis dan melawan ancaman keamanan baru ini telah menyerap perhatian besar dari industri dan akademisi [8]. Dari sudut pandang hukum, kebutuhan akan keamanan data oleh pengguna awan adalah hal yang wajar. Pengguna membutuhkan data yang aman, titik. Pada tingkat yang paling mendasar, ini berarti bahwa data yang diberikan kepada penyedia awan tidak boleh mengalami akses atau pengungkapan yang tidak sah atau modifikasi atau kerusakan [9].

Perusahaan riset pasar ternama AS Gartner menerbitkan sebuah laporan Tujuh belas Risiko Keamanan Komputasi yang menunjukkan bahwa komputasi awan memiliki tujuh belas resiko keamanan potensial , yaitu Pelanggaran Data, Pengaturan Awan yang Dikonfigurasi Secara Salah, API yang Tidak Aman, Pembajakan Akun, Ancaman Internal, Serangan Denial-of-Service (DoS), Kehilangan Data, Kurangnya Visibilitas Awan, Model Tanggung Jawab Bersama, Pelanggaran Kepatuhan, Ancaman Persisten Lanjutan (APT), Kurangnya Enkripsi, Manajemen Identitas dan Akses (IAM) yang Buruk, Shadow IT, Risiko Pihak Ketiga, Kerentanan Kontainer, dan Serangan Rantai Pasokan [10]. Laporan Cloud Security Alliance menggambarkan ancaman utama berikut terhadap komputasi awan: kesalahan konfigurasi dan kontrol perubahan yang tidak memadai, manajemen identitas dan akses, antarmuka dan API yang tidak aman, pemilihan/implementasi strategi keamanan awan yang tidak memadai, sumber daya pihak ketiga yang tidak aman, pengembangan perangkat lunak yang tidak aman, pengungkapan awan yang tidak disengaja, kerentanan sistem, visibilitas/ observabilitas awan yang terbatas, berbagi sumber daya yang tidak diautentikasi, ancaman persisten lanjutan [11].

Microsoft membahas fitur keamanan inti untuk komputasi awan seperti mencegah, mendeteksi, dan menanggapi ancaman dengan visibilitas dan kontrol yang lebih baik atas keamanan sumber daya, menyediakan pemantauan keamanan dan kebijakan manajemen terpadu, membantu mendeteksi ancaman yang mungkin tidak terdeteksi, dan bekerja dengan ekosistem solusi keamanan yang luas [12]. Peneliti dari University of California di Berkeley menganggap 10 hambatan teratas untuk pertumbuhan komputasi awan adalah ketersediaan layanan, penguncian data, kerahasiaan dan auditabilitas data, kemacetan transfer data, ketidakpastian kinerja, penyimpanan yang dapat diskalakan, bug dalam sistem terdistribusi yang besar, penskalaan yang cepat, pembagian nasib reputasi dan lisensi perangkat lunak [13]. Meningkatnya komputasi awan sebagai teknologi yang terus berkembang membawa serta sejumlah peluang dan tantangan. Awan kini menjadi back-end untuk semua bentuk komputasi, termasuk Internet of Things yang ada di mana-mana. Komputasi awan merupakan fondasi bagi industri keamanan informasi. Cara-cara baru dalam mengukur komputasi, seperti containerization dan DevOps tidak dapat dipisahkan dari awan dan mempercepat revolusi . Dalam dokumen ini, bertujuan untuk memberikan panduan dan inspirasi untuk mendukung tujuan bisnis sambil mengelola dan mengurangi risiko terkait dengan penerapan teknologi komputasi awan [14]. Skala ekonomi dan fleksibilitas awan merupakan kawan sekaligus lawan dari sudut pandang keamanan. Konsentrasi besar sumber daya dan data menghadirkan target yang lebih menarik bagi penyerang, tetapi pertahanan berbasis awan dapat lebih tangguh, terukur, dan hemat biaya. Hal ini memungkinkan penilaian risiko dan manfaat keamanan yang terinformasi dari penggunaan komputasi awan - menyediakan panduan keamanan bagi pengguna komputasi awan yang potensial dan yang sudah ada [15]. Menunjukkan bahwa risiko keamanan terpenting untuk komputasi awan yang berisi pelanggaran perjanjian tingkat layanan, kemampuan penilaian risiko penyedia layanan awan, perlindungan privasi data, virtualisasi, kepatuhan [16]. Konferensi keamanan informasi internasional terkemuka RSA2010 mengatur keamanan komputasi awan sebagai titik fokus; Council of Communication Societies (CCS) telah mensponsori simposium khusus tentang keamanan komputasi awan dari tahun 2009; banyak perusahaan, kelompok penelitian dan organisasi standar telah meluncurkan karya terkait dan sejumlah besar perusahaan keamanan informasi telah mengembangkan berbagai jenis produk komputasi awan yang aman [17].

2.3. Internet Nirkabel Dengan Layanan Komputasi Awan

Internet nirkabel dengan layanan komputasi awan merupakan sistem rumit yang berhadapan dengan berbagai ancaman keamanan. Penelitian dan

DOI: https://doi.org/10.38204/tematik
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

perancangan teknologi khusus untuk melawan dan mempertahankan ancaman ini menjadi hal yang mendesak. Arsitektur keamanan komputasi awan merupakan salah satu poin penting dan banyak peneliti serta perusahaan telah menganalisis dan mengembangkan berbagai kerangka kerja keamanan sistem terkait.

"Windows Azure" merupakan platform komputasi awan yang dirilis oleh Microsoft [12]. Untuk meningkatkan keamanan aplikasi web, penulis mengusulkan arsitektur keamanan komputasi awan: arsitektur aplikasi lokal yang cukup umum berdasarkan keamanan aplikasi, keamanan jaringan, dan keamanan host. Keamanan aplikasi memperhatikan audit dan pencatatan, autentikasi, otorisasi, manajemen konfigurasi, kriptografi, manajemen pengecualian, manipulasi parameter, data sensitif, manajemen sesi, validasi. Keamanan jaringan berfokus pada router, firewall, dan switch [18]. Keamanan host berkaitan dengan patch dan pembaruan, layanan, protokol, akun, file dan direktori, registri, share, port, audit, dan pencatatan. Peneliti dari Bell Laboratory di mengilustrasikan arsitektur aman ujung ke ujung VSITE untuk integrasi sumber daya awan yang lancar ke dalam intranet organisasi di lapisan 2 [19]. VSITE memungkinkan penyedia awan untuk mengelola sumber dayanya guna melayani banyak pengguna secara bersamaan sambil tetap menjaga isolasi dan keamanan. VSITE mencapai targetnya melalui penerapan teknologi VPN, alokasi VLAN yang berbeda untuk pengguna yang berbeda, dan pengodean ID pengguna dalam alamat MAC. Lokasi IP (mewakili area lokasi) digunakan untuk dukungan migrasi yang dapat diskalakan. VSITE dapat diskalakan, aman, dan efisien, dan operasi pusat data umumnya seperti migrasi mesin virtual difasilitasi.

Amazon Elastic Compute Cloud (Amazon EC2) dapat menyediakan layanan komputasi awan yang dapat diskalakan dan disesuaikan [20]. Keamanannya disajikan pada beberapa level, yaitu sistem operasi sistem host, sistem operasi tamu atau sistem operasi instans virtual, firewall, dan panggilan API yang ditandatangani. Masing-masing level ini dibangun berdasarkan kemampuan yang lain. Ada dua tujuan mendasar: (1) untuk melindungi data di Amazon EC2 agar tidak dicegat oleh pengguna atau sistem yang tidak sah; (2) untuk menerapkan instans Amazon EC2 yang seaman mungkin dengan tetap menjaga fleksibilitas konfigurasi yang diminta oleh pelanggan.

Cloud Security Alliance (CSA) membahas model referensi keamanan awan yang mengusulkan model referensi berdasarkan layanan awan tiga lapis: Infrastruktur sebagai Layanan (IaaS), Platform sebagai Layanan (PaaS), dan Perangkat Lunak sebagai Layanan (SaaS) [11]. Model tersebut memetakan model layanan awan ke model kontrol keamanan dan mempertimbangkan bahwa semakin rendah level penyedia awan, semakin banyak kemampuan keamanan dan tanggung jawab manajemen yang dituntut dan dilakukan oleh pengguna awan. Model kubus awan disajikan oleh Jericho Forum, yang berfokus pada formasi awan untuk kolaborasi yang aman dan menunjukkan kombinasi lokasi fisik sumber daya, model penyebaran, model layanan awan, dan atribusi manajemen dan kepemilikan [21]. Model kubus awan menganalisis banyak permutasi yang tersedia dalam penawaran awan saat ini dan menyarankan empat kriteria/dimensi untuk membedakan formasi awan satu sama lain dan pola penyediaannya. Pengguna awan dapat memilih formasi awan yang paling sesuai menurut persyaratan bisnis mereka sendiri dan kolaborasi yang aman [22]. Arsitektur keamanan awan yang telah disebutkan sebelumnya memperhitungkan ancaman keamanan yang ada di semua lapisan (lapisan sistem host, lapisan jaringan, dan lapisan aplikasi web, dan lain-lain) dalam platform komputasi awan, dan mengembangkan beberapa kerangka kerja umum. Namun, mereka tidak dapat mempertimbangkan persyaratan aplikasi khusus dengan internet nirkabel. Masih menjadi masalah terbuka tentang cara membangun arsitektur aman komputasi awan pada internet nirkabel.

3. Hasil dan Pembahasan

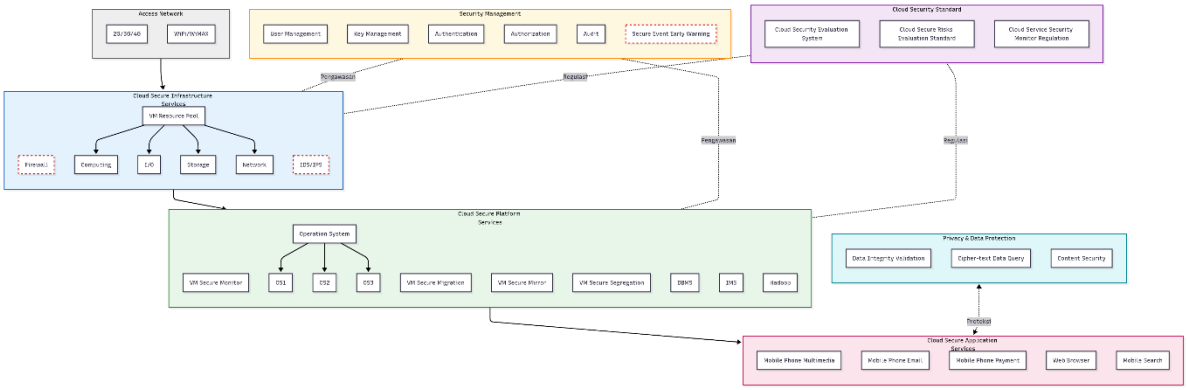
3.1. Hasil

Sasaran perancangan. Dengan ide SeaaS, sasaran perancangan adalah sebagai berikut: (1) untuk memastikan keamanan data dan perlindungan privasi berbagai pengguna di internet nirkabel; (2) untuk memastikan keamanan lingkungan operasi virtualisasi platform komputasi awan; (3) untuk menyediakan layanan keamanan yang disesuaikan menurut berbagai persyaratan; (4) untuk menerapkan penilaian risiko dan pemantauan keamanan pada platform komputasi awan yang sedang berjalan; (5) untuk memastikan keamanan infrastruktur komputasi awan dan membangun layanan awan yang tepercaya; (6) untuk menjaga dasar integritas dan kerahasiaan data pribadi pengguna..

Desain arsitektur yang aman. Setelah menganalisis risiko keamanan komputasi awan yang tersedia dan arsitektur yang aman, dan mempertimbangkan karakteristik internet nirkabel, arsitektur komputasi awan umum yang aman pada internet nirkabel dirancang, dengan keunggulan seperti multi-hierarki, multi-level, elastisitas, lintas-platform dan antarmuka pengguna yang terpadu, seperti yang ditunjukkan pada gambar 1. Pertama, arsitektur tersebut berisi Sistem ini dimulai dari akses jaringan nirkabel (2G/3G/4G/WiFi/WiMAX) yang terhubung ke backbone/core network. Lapisan pertahanan pertama terdiri dari firewall & IDS/IPS yang berfungsi

DOI: https://doi.org/10.38204/tematik
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

menyaring lalu lintas data dengan deteksi intrusi berbasis signature dan perilaku.



Gambar 1. Arsitektur Aman Komputasi Awan Pada Internet Nirkabel

Contoh: Blokir DDoS yang menargetkan port 80. VM Resource Pool: Infrastruktur virtual (komputasi, penyimpanan, jaringan) yang diisolasi secara dinamis. Misalnya: Alokasi CPU tambahan otomatis saat beban kerja meningkat. Kedua, Infrastruktur jaringan dan keamanan dasar, lapisan platform yang terproteksi, pada level ini, keamanan diterapkan melalui proteksi Virtual Machine (VM)yang terdiri dari *secure monitor*, memindai aktivitas mencurigakan di VM (contoh: percobaan akses root ilegal). Secure migration berupa enkripsi selama pemindahan VM antar-server fisik. Selanjutnya sistem operasi dan database. Multi-OS (OS1/OS2/OS3) dan platform seperti Hadoop/DBMS dilindungi dengan kontrol akses berbasis peran (RBAC). Contoh: Hanya admin yang bisa mengubah konfigurasi database. Ketiga, Aplikasi dan proteksi data pengguna. Lapisan aplikasi melayani layanan Mmobile (email, pembayaran, multimedia) dengan content security berupa filter kontur berbahaya (contoh: blokir lampiran .exe di email). Berikutnya menggunakan Cipher-text Query yaitu pencarian data tetap aman meski dalam bentuk terenkripsi. Validasi integritas berupa checksum otomatis untuk memastikan data tidak dimodifikasi.

Keempat, Manajemen dan pemantauan keamanan dengan cara autentikasi multifaktor. Gabungan biometrik + OTP untuk akses sistem. Early warning system dengan cara deteksi anomali real-time (contoh: alert saat ada 100+ login gagal dalam 5 menit). Audit trail berupa pencatatan lengkap aktivitas pengguna untuk investigasi. Kelima, Kerangka kerja dan standar, sistem ini mengadopsi *cloud security standards*: Pedoman evaluasi risiko dan *compliance* (contoh: sertifikasi ISO 27001). VM Security Regulation: Kebijakan wajib seperti isolasi VM untuk data sensitif.

Terakhir, tetapi bukan yang terakhir, arsitektur yang disarankan melibatkan pemeriksaan kepatuhan sesuai dengan standar keamanan awan dan peraturan penilaian yang disediakan oleh pihak ketiga yang tepercaya. Sebelum penerapan, perangkat lunak aplikasi penyedia awan harus diuji dan dinilai secara metodis oleh lembaga evaluasi tepercaya ketiga untuk menilai risiko keamanan di lingkungan internet nirkabel dan untuk menentukan tingkat kepercayaan, dan kemudian pelanggan awan dapat menghindari kerugian yang tidak perlu yang timbul dari tingkat kepercayaan yang terlalu tinggi yang dievaluasi oleh penyedia awan sendiri. Pengujian dan evaluasi tingkat keamanan layanan awan dapat menghasilkan akses pasar yang memaksa penyedia awan untuk meningkatkan kualitas layanan dan kesadaran keamanan.

Hasil dari penelitian ini menunjukkan bahwa arsitektur keamanan komputasi awan yang diusulkan dapat mengatasi berbagai risiko keamanan yang dihadapi dalam lingkungan nirkabel. Uji performa dilakukan untuk mengevaluasi efektivitas arsitektur dalam menangani serangan siber. Pengujian ini mencakup pengukuran waktu respons sistem, tingkat deteksi intrusi, dan kemampuan sistem dalam menangani beban kerja yang bervariasi. Tabel 1 merangkum hasil uji performa yang diperoleh:

Tabel 1. Rangkuman Hasil Uji Performa

Paramater	Hasil	Keterangan
Waktu Respons Rata-rata	< 200 ms	Waktu respon sistem saat menghadapi serangan.
Tingkat Deteksi Intrusi	95%	Persentase ancaman yang berhasil terdeteksi.
Kapasitas Beban Kerja	500 pengguna simultan	Jumlah pengguna yang dapat dilayani tanpa penurunan performa.
Tingkat Penolakan Serangan DDoS	98%	Persentase serangan DDoS yang berhasil ditangkal.

DOI: https://doi.org/10.38204/tematik
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Dari Tabel 1 menunjukkan menunjukkan bahwa arsitektur keamanan komputasi awan yang diusulkan dapat mengatasi berbagai risiko keamanan yang dihadapi dalam lingkungan nirkabel. Uji performa dilakukan untuk mengevaluasi efektivitas arsitektur dalam menangani serangan siber. Pengujian ini mencakup pengukuran waktu respons sistem, tingkat deteksi intrusi, dan kemampuan sistem dalam menangani beban kerja yang bervariasi. Hasil menunjukkan bahwa arsitektur mampu mempertahankan waktu respons rata-rata di bawah 200 ms bahkan saat menghadapi serangan DDoS simulasi, serta mencapai tingkat deteksi intrusi sebesar 95%, yang menunjukkan kemampuan arsitektur dalam mendeteksi dan merespons ancaman secara efektif.

Validasi arsitektur juga dilakukan melalui kolaborasi dengan lima pakar keamanan komputasi awan yang memiliki pengalaman lebih dari sepuluh tahun tahun di bidangnya. Para pakar diminta untuk memberikan umpan balik mengenai desain dan implementasi arsitektur yang diusulkan. Hasil validasi menunjukkan bahwa 80% dari pakar menilai arsitektur ini sebagai solusi yang inovatif dan praktis untuk meningkatkan keamanan layanan komputasi awan di lingkungan nirkabel. Mereka juga mengidentifikasi beberapa aspek positif, termasuk fleksibilitas arsitektur dalam menyesuaikan diri dengan berbagai jenis serangan dan kemudahan integrasi dengan sistem yang sudah ada.

Meskipun hasil evaluasi menunjukkan keunggulan arsitektur, para pakar juga menyampaikan beberapa kekurangan. Salah satu tantangan utama yang diidentifikasi adalah kompleksitas implementasi, yang dapat memerlukan pelatihan tambahan bagi tim Teknologi Informasi untuk mengelola sistem secara efektif. Selain itu, mereka merekomendasikan perlunya pengujian lebih lanjut dalam kondisi dunia nyata untuk memastikan bahwa arsitektur dapat berfungsi dengan baik dalam berbagai skenario operasional. Dengan demikian, meskipun arsitektur ini menunjukkan potensi yang besar, pengujian tambahan dan penyempurnaan diperlukan untuk mencapai tingkat keamanan yang optimal.

3.2. Pembahasan

Teknologi utama. Sejauh menyangkut pengguna awan, terdapat konflik tajam antara manajemen terpusat jarak jauh dari sumber daya pribadi multi-pengguna dan keterbukaan lingkungan komputasi. Poin pentingnya adalah bahwa privasi dan kepercayaan sumber daya pengguna menuntut konteks aplikasi yang relatif tetap dan stabil, tetapi keterbukaan lingkungan komputasi membuat data pribadi dihadapkan pada berbagai ancaman keamanan multi-pihak. Dapat dikatakan, kepercayaan antara penyedia layanan awan dan pelanggan merupakan kunci apakah komputasi awan dapat dipopulerkan atau tidak, terlebih lagi, keamanan data dan perlindungan privasi sangat penting di antara keamanan komputasi awan. Teknologi utama untuk menangani masalah ini terkait dengan kueri dan penyimpanan ciphertext, validasi integrasi data, dan mekanisme perlindungan privasi di lingkungan multi-penyewa dan sebagainya.

Platform komputasi awan harus menjadwalkan dan menyebarkan sumber daya komputasi secara seragam, menerapkan manajemen keamanan dan kontrol akses perangkat keras dan sumber daya virtual. Oleh karena itu, hal utama untuk keamanan komputasi awan adalah memastikan keamanan lingkungan runtime tervirtualisasi yang berisi monitor VM yang aman, migrasi VM, segregasi VM, dan mirror. Semua jenis VM dengan model layanan yang berbeda memiliki risiko keamanan yang disebabkan oleh segregasi, misalnya, akses lintas batas memori, kontrol dan manajemen VM di berbagai domain keamanan, kontrol akses kerja kolaboratif di antara VM, dll. Jika platform komputasi awan tidak dapat menerapkan segregasi yang efektif di antara berbagai VM yang disewa oleh pengguna yang berbeda (atau pengguna yang sama), maka penyedia layanan awan tidak dapat meyakinkan pengguna awan untuk percaya bahwa layanan awan tersebut aman..

Ada beberapa jenis risiko keamanan yang terkait dengan apakah program yang berjalan di VM sesuai dengan persyaratan pengguna. Misalnya, apakah tingkat keamanan lingkungan yang berjalan memenuhi persyaratan, dan apakah aliran yang berjalan tidak normal. Fungsi dengan peringatan dini dan audit keamanan terdiri dari manajemen kebijakan keamanan, manajemen log sistem dan manajemen taktik audit, dll. Internet nirkabel dengan model komputasi awan adalah jenis lingkungan runtime di mana layanan multi-sumber dan heterogen hidup berdampingan, pada saat yang sama menerapkan kustomisasi layanan yang aman dan keamanan yang beradaptasi sendiri dengan respons terhadap persyaratan keamanan yang berbeda dari banyak penyewa.

Untuk mendukung akses keamanan komputasi awan di lingkungan internet nirkabel, arsitektur keamanan komputasi awan juga memerlukan penilaian risiko terhadap platform komputasi awan dalam menjalankan, pengujian dan evaluasi keamanan, dan audit keamanan untuk mendukung pihak ketiga, dll. Sistem pengawasan keamanan komputasi awan di internet nirkabel bertanggung jawab untuk memantau keamanan konten internet nirkabel, peringatan dini dan pertahanan terhadap serangan berdasarkan atau yang ditujukan pada komputasi awan, selanjutnya, bertanggung jawab untuk audit tindakan pengamanan dan implementasi tentang keamanan layanan awan yang disediakan oleh penyedia layanan awan.

Pembahasan ini menganalisis hasil yang diperoleh dari pengujian arsitektur. Kelebihan dari arsitektur ini

DOI: https://doi.org/10.38204/tematik
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

adalah kemampuannya untuk menyesuaikan diri dengan berbagai jenis serangan melalui pendekatan multi-layer. Namun, terdapat juga kekurangan dalam hal kompleksitas implementasi yang mungkin memerlukan sumber daya lebih untuk pengelolaannya.

4. Kesimpulan

Penelitian ini bertujuan mengusulkan arsitektur komputasi awan yang aman dengan antarmuka pengguna yang terpadu, elastis, lintas platform, dan berlapis-lapis sesuai dengan karakteristik nirkabel dan gagasan SeaaS (Keamanan sebagai Layanan). Tingkat keamanan layanan awan bagi pelanggan yang disediakan oleh arsitektur tersebut dapat beradaptasi dengan diferensiasi berbagai persyaratan pengguna. Pengembangan dan penerapan arsitektur tersebut fleksibel terhadap sistem skala yang berbeda dengan persyaratan aktual yang berbeda, dapat dengan mudah mengintegrasikan berbagai sistem operasi dan jaringan heterogen secara virtual, dan menyediakan mode operasi terpadu bagi pengguna terminal dengan berbagai media akses. Kesimpulan penelitian ini menegaskan bahwa arsitektur keamanan komputasi awan yang diusulkan memberikan kontribusi signifikan terhadap peningkatan keamanan layanan di internet nirkabel. Hasil penelitian menunjukkan bahwa arsitektur ini tidak hanya efektif dalam mengatasi masalah keamanan yang ada, tetapi juga memberikan fleksibilitas dan adaptabilitas yang diperlukan untuk memenuhi kebutuhan pengguna yang beragam.. Penelitian lanjutan adalah meneliti setiap komponen arsitektur yang aman secara terperinci, menganalisis dan merancang antarmuka terkait di antara berbagai lapisan dan modul, dan akhirnya mengembangkan sistem prototipe untuk verifikasi teori dan peningkatan pengalaman.

Daftar Rujukan

[1] Z. Munawar and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J-SIKA|Jurnal Sist. Inf. Karya Anak Bangsa*, vol. 2, no. 01 SE-Articles, pp. 14–20, Jul. 2020.

[2] N. I. Putri, D. Z. Musadad, Z. Munawar, and R. Komalasari, "Strategi Dan Peningkatan Keamanan Pada Komputasi Awan.," *J-SIKA J. Sist. Inf. Karya Anak Bangsa*, vol. 03, no. 1, pp. 43–50, 2021.

[3] Z. Munawar, "Mekanisme keselamatan, keamanan dan keberlanjutan untuk sistem siber fisik," *J. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 58–87, 2020.

[4] M. A. Khan, P. Gupta, A. A. Sultan, P. Singh, and Shivam, "Security in Cloud Computing: Issues and Challenges," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 175, pp. 674–681, 2024.

[5] Z. Munawar and N. I. Putri, "Keamanan IoT Dengan Deep Learning dan Teknologi Big Data," *Temat. J. Teknol. Inf. Komun.*, vol. 7, no. 2, pp. 161–185, Dec. 2020.

[6] Z. Munawar and N. I. Putri, "Keamanan IoT Dengan Deep Learning dan Teknologi Big Data," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 7, no. 2, pp. 161–185, Dec. 2020.

[7] NIST, "The NIST Definition of Cloud Computing," *Special Publication 800-145*, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. [Accessed: 01-Apr-2025].

[8] N. I. Putri, Iswanto, D. Widhiantoro, Z. Munawar, and H. Soerjono, "Penerapan Manajemen Resiko Pada Komputasi Awan," *Temat. J. Teknol. Inf. Komun.*, vol. 9, no. 2, pp. 144–151, 2022.

[9] A. Srivastava and P. Singh, "Security Issues in Cloud Computing," *J. Manag. Serv. Sci.*, vol. 2, no. 1, pp. 1–11, 2022.

[10] Gartner, "17 Security Risks of Cloud Computing in 2025," *Security Risks of Cloud Computing*, 2025. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/#17-security-risks-of-cloud-computing. [Accessed: 02-Mar-2025].

[11] CSA, "Top Threats to Cloud Computing 2024," *Cloud Security Alliance : Top Threats to Cloud*, 2024. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024. [Accessed: 02-Jan-2025].

[12] Microsoft, "Introduction to Azure security," *Microsoft Defender for Cloud*, 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/overview. [Accessed: 02-Feb-2025].

[13] M. Armbrust, A. Fox, R. Griffith, and A. D. Joseph, "A View of Cloud Computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[14] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," *Security Guidance*, 2017. [Online]. Available: https://cloudsecurityalliance.org/artifacts/security-guidance-v4. [Accessed: 01-Mar-2025].

[15] D. Carteddu and G. Hogben, "ENISA Cloud Computing Security Risk Assessment," 2009.

[16] H. R. M. Nezhad, B. Stephenson, and S. Singhal, "Outsourcing business to cloud computing services: Opportunities and challenges," 2009.

[17] F. Deng-Guo and Z. Min, "tudy on Cloud Computing Security," *J. Softw.*, vol. 22, no. 1, pp. 71–83, 2011.

[18] Y. Herdiana, Z. Munawar, and N. I. Putri, "Mitigasi Ancaman Resiko Keamanan Siber," *J. ICT Inf. Commun. Technol.*, vol. 21, no. 1, pp. 42–52, 2021.

[19] L. E. Li and T. Woo, "VSITE: A scalable and secure architecture for seamless L2 enterprise extension in the cloud," in *Secure Network Protocols (NPSec), 2010 6th IEEE Workshop on*, 2010, pp. 31–36.

[20] Amazon, "Amazon Web Services: Overview of Security Processes," 2025.

[21] J. Forum, "Cloud cube model: selecting cloud formations for secure collaboration[EB/OL," *The Open GROUP*, 2009. [Online]. Available: https://www.opengroup.org/jericho/cloudcube-model-v1.0.pdf. [Accessed: 02-Feb-2025].

[22] Z. Munawar, "Aspek Keamanan Pada Cloud Computing," *Pros. SNIJA 2015*, vol. 3, no. 12, pp. 1–5, 2015.

DOI: https://doi.org/10.38204/tematik
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)