

PENGEMBANGAN INFRASTRUKTUR HOSTING MOBILE MENGUNAKAN MICROSERVER BERBASIS VIRTUAL MACHINE DAN MODEL KEAMANAN ZERO TRUST

Moch Rafli Muchibbin, Arda Surya Editya, Neny Kurniati

Informatika, Universitas Nahdlatul Ulama Sidoarjo

Jalan Lingkar Timur KM 5,5 Rangkah Kidul Sidoarjo, Indonesia

speedrafl64@gmail.com

ABSTRAK

Perkembangan layanan digital membutuhkan infrastruktur server yang fleksibel, aman, dan efisien untuk mendukung kebutuhan hosting modern. Permasalahan yang sering muncul pada server konvensional meliputi biaya implementasi yang tinggi, konsumsi daya besar, serta keterbatasan dalam pengelolaan keamanan dan mobilitas sistem. Penelitian ini bertujuan mengembangkan infrastruktur hosting mobile menggunakan microserver berbasis virtual machine dengan penerapan model keamanan Zero Trust. Metode penelitian yang digunakan adalah Research and Development (R&D) dengan tahapan perancangan sistem, implementasi infrastruktur, konfigurasi virtual machine, penerapan keamanan Zero Trust, dan pengujian layanan hosting. Sistem dibangun menggunakan server virtual berbasis Ubuntu yang dijalankan pada lingkungan virtualisasi untuk mendukung pengelolaan sumber daya secara fleksibel dan terstruktur. Model keamanan Zero Trust diterapkan melalui proses verifikasi akses secara berkelanjutan untuk meningkatkan perlindungan sistem. Hasil penelitian menunjukkan bahwa kombinasi microserver, virtual machine, dan Zero Trust mampu menghasilkan sistem hosting mobile yang lebih aman, efisien, hemat daya, serta adaptif dalam mendukung kebutuhan layanan digital.

Kata kunci : *microserver, virtual machine, Zero Trust, hosting mobile, keamanan jaringan, virtualisasi*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong peningkatan kebutuhan terhadap infrastruktur komputasi yang efisien, aman, dan mudah dikelola. Berbagai institusi pendidikan, organisasi, maupun komunitas pengembang saat ini membutuhkan layanan hosting yang mampu mendukung akses aplikasi secara cepat dan stabil, termasuk untuk layanan berbasis perangkat bergerak. Dalam konteks tersebut, infrastruktur server konvensional sering kali menghadapi sejumlah kendala, seperti kebutuhan biaya yang relatif tinggi, konsumsi daya yang besar, keterbatasan fleksibilitas pengelolaan, serta kompleksitas dalam pengamanan akses layanan [1].

Kondisi ini mendorong perlunya alternatif infrastruktur yang lebih ringkas, hemat sumber daya, namun tetap mampu memberikan performa dan keamanan yang memadai.

Salah satu pendekatan yang dapat digunakan adalah pemanfaatan microserver. Microserver merupakan server berukuran kecil dengan konsumsi daya rendah yang dirancang untuk menangani layanan komputasi tertentu secara efisien [2].

Dibandingkan dengan server tradisional, microserver memiliki keunggulan dalam hal efisiensi energi, kebutuhan ruang yang lebih kecil, dan biaya implementasi yang lebih terjangkau [3].

Meskipun teknologi microserver dan virtualisasi menawarkan berbagai keunggulan, implementasi layanan hosting skala kecil hingga menengah masih menghadapi beberapa kendala. Infrastruktur server konvensional memerlukan biaya implementasi dan

operasional yang relatif tinggi serta membutuhkan pengelolaan keamanan yang kompleks. Selain itu, layanan hosting yang terhubung ke jaringan publik rentan terhadap ancaman keamanan siber, seperti akses tidak sah, eksploitasi layanan, dan pencurian data [7].

Di sisi lain, banyak implementasi hosting mandiri masih berfokus pada aspek performa dan efisiensi tanpa mengintegrasikan pendekatan keamanan modern secara menyeluruh.

Penelitian ini bertujuan untuk merancang dan mengimplementasikan infrastruktur hosting mobile berbasis microserver dengan dukungan virtual machine, serta menerapkan model keamanan Zero Trust untuk meningkatkan keamanan akses layanan. Selain itu, penelitian ini juga bertujuan untuk menguji fungsi dasar infrastruktur yang dibangun dalam mendukung layanan hosting mobile secara fleksibel, efisien, dan aman. Meskipun demikian, peningkatan fleksibilitas infrastruktur digital juga diikuti oleh meningkatnya risiko keamanan siber [7].

Sistem hosting yang terhubung ke jaringan rentan terhadap berbagai ancaman, seperti akses tidak sah, pencurian data, eksploitasi celah layanan, serta penyalahgunaan identitas pengguna atau perangkat [8].

Salah satu model keamanan yang banyak dikembangkan untuk menjawab tantangan tersebut adalah Zero Trust. Prinsip utama Zero Trust adalah “never trust, always verify,” yaitu tidak memberikan kepercayaan otomatis kepada pengguna, perangkat, maupun sistem meskipun berada di dalam jaringan internal [9].

Setiap permintaan akses harus diverifikasi secara ketat berdasarkan identitas, otorisasi, dan konteks akses yang berlaku. Penerapan model ini dinilai mampu meningkatkan kontrol keamanan, mengurangi potensi pergerakan lateral serangan di dalam sistem, serta memperkuat perlindungan terhadap layanan hosting yang diakses secara daring. Dengan demikian, integrasi Zero Trust pada infrastruktur microserver berbasis virtual machine menjadi pendekatan yang relevan untuk menghasilkan sistem hosting yang tidak hanya efisien tetapi juga lebih aman [10].

Dengan menggabungkan microserver, virtualisasi, dan Zero Trust, penelitian ini diharapkan dapat memberikan solusi yang lebih komprehensif dalam membangun layanan hosting mobile [11].

Hasil dari penelitian ini diharapkan dapat memberikan kontribusi praktis sebagai alternatif pengembangan infrastruktur server skala kecil yang hemat biaya dan efisien, sekaligus memberikan kontribusi akademik dalam penerapan konsep virtualisasi dan keamanan Zero Trust pada lingkungan hosting [12].

Penyelesaian masalah dalam penelitian ini dilakukan melalui pembangunan infrastruktur microserver berbasis virtual machine yang dikonfigurasi sebagai layanan hosting mobile. Selanjutnya, model keamanan Zero Trust diterapkan untuk mengatur proses autentikasi dan kontrol akses terhadap layanan yang berjalan pada server. Pengujian dilakukan terhadap fungsi dasar layanan hosting, konektivitas sistem, serta mekanisme keamanan akses guna mengetahui kemampuan sistem dalam mendukung layanan hosting yang aman dan efisien. Dengan demikian, penelitian ini memiliki relevansi yang kuat baik dari sisi pengembangan teknologi maupun dari sisi kebutuhan implementatif di berbagai lingkungan yang memerlukan layanan hosting mandiri dengan tingkat keamanan yang lebih baik [13].

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian terdahulu digunakan sebagai landasan dalam pengembangan penelitian mengenai implementasi hosting mobile berbasis microserver dengan dukungan virtual machine dan keamanan Zero Trust. Beberapa penelitian yang relevan menunjukkan bahwa teknologi microserver mampu digunakan sebagai alternatif server hosting dengan biaya rendah namun tetap memiliki performa yang baik.

Penelitian yang dilakukan oleh Muhammad Syahrul Fikri dan Asep Tedyyana pada jurnal JATI (Jurnal Mahasiswa Teknik Informatika) membahas mengenai rancang bangun sistem hosting mandiri menggunakan Raspberry Pi dan aaPanel sebagai solusi alternatif web hosting murah [1].

Hasil penelitian menunjukkan bahwa Raspberry Pi dapat dimanfaatkan sebagai server hosting mandiri dengan konsumsi daya rendah dan biaya operasional yang lebih hemat dibandingkan server konvensional. Penelitian tersebut menjadi acuan dalam penggunaan

perangkat microserver sebagai infrastruktur hosting pada penelitian ini.

Selanjutnya, penelitian oleh A. S. Editya, C. Lega, dan U. USSADA membahas kinerja microserver dalam menangani lalu lintas berat pada dedicated host server untuk jaringan lokal [2].

Penelitian tersebut menunjukkan bahwa microserver mampu mempertahankan performa layanan meskipun menerima beban trafik yang tinggi. Hasil tersebut mendukung pemanfaatan microserver sebagai media hosting yang stabil dan efisien.

Penelitian serupa juga dilakukan oleh A. S. Editya dan N. Kurniati pada konferensi IEEE International Conference on Communication, Networks and Satellite [3].

Penelitian tersebut menguji performa microserver dalam menangani heavy traffic pada dedicated server host berbasis Local Area Network (LAN). Hasil penelitian menunjukkan bahwa microserver memiliki kemampuan yang cukup baik dalam menjaga kestabilan layanan jaringan dan distribusi trafik server.

Berdasarkan beberapa penelitian terdahulu tersebut, dapat disimpulkan bahwa microserver memiliki potensi besar sebagai solusi infrastruktur hosting yang efisien dan ekonomis. Namun, pada penelitian sebelumnya belum banyak diterapkan integrasi virtual machine serta pendekatan keamanan berbasis Zero Trust dalam satu sistem hosting mobile. Oleh karena itu, penelitian ini dikembangkan dengan menambahkan implementasi virtualisasi server menggunakan Ubuntu pada lingkungan virtual machine serta penerapan model keamanan Zero Trust untuk meningkatkan keamanan akses dan fleksibilitas sistem hosting.

2.2. Metode

Penelitian ini menggunakan pendekatan Research and Development (R&D) yang difokuskan pada proses perancangan, pembangunan, implementasi, dan pengujian infrastruktur hosting mobile berbasis microserver dengan dukungan teknologi virtual machine serta penerapan model keamanan Zero Trust. Pendekatan ini dipilih karena penelitian tidak hanya bertujuan untuk mendeskripsikan suatu fenomena, tetapi juga menghasilkan suatu sistem yang dapat diuji secara langsung pada lingkungan implementasi nyata. Melalui metode ini, penelitian diarahkan untuk menghasilkan rancangan infrastruktur yang efisien, fleksibel, dan aman dalam mendukung layanan hosting [14].

Setiap tahapan dilakukan secara bertahap agar sistem yang dibangun dapat memenuhi kebutuhan fungsional maupun kebutuhan keamanan [15].

2.3. Jenis dan Pendekatan Penelitian

Jenis penelitian ini adalah penelitian terapan dengan pendekatan eksperimental. Penelitian terapan digunakan karena hasil akhir penelitian berupa

implementasi sistem yang dapat dimanfaatkan secara langsung sebagai infrastruktur hosting mobile. Sementara itu, pendekatan eksperimental digunakan untuk menguji bagaimana kombinasi microserver, virtual machine, dan model keamanan Zero Trust dapat bekerja dalam satu lingkungan sistem yang terintegrasi.

Penelitian ini menekankan pada pembangunan sebuah server virtual berbasis Ubuntu yang dijalankan di atas sistem operasi Windows menggunakan aplikasi virtualisasi. Lingkungan virtual tersebut kemudian dikonfigurasi untuk menjalankan layanan hosting sekaligus menerapkan pembatasan akses berbasis prinsip never trust, always verify.

3. METODE PENELITIAN

3.1. Rancangan Sistem

Rancangan sistem dalam penelitian ini menempatkan Windows sebagai sistem operasi utama (host), kemudian di atasnya dijalankan aplikasi virtualisasi untuk membuat sebuah virtual machine dengan sistem operasi Ubuntu. Ubuntu berfungsi sebagai server virtual yang digunakan untuk menjalankan layanan hosting mobile. Dengan model ini, seluruh layanan inti ditempatkan pada lingkungan virtual sehingga lebih mudah dikelola, diuji, dan diisolasi dari sistem utama.

Dalam rancangan ini, pengguna mengakses layanan melalui jaringan menuju server virtual Ubuntu. Sebelum akses diberikan, sistem menerapkan kebijakan keamanan berbasis Zero Trust, yaitu setiap pengguna, perangkat, dan permintaan koneksi harus diverifikasi terlebih dahulu. Dengan demikian, sistem tidak hanya berfokus pada penyediaan layanan hosting, tetapi juga memperkuat kontrol keamanan terhadap seluruh proses akses.

3.2. Tahapan Penelitian

Tahapan penelitian dilakukan secara sistematis sebagai berikut:

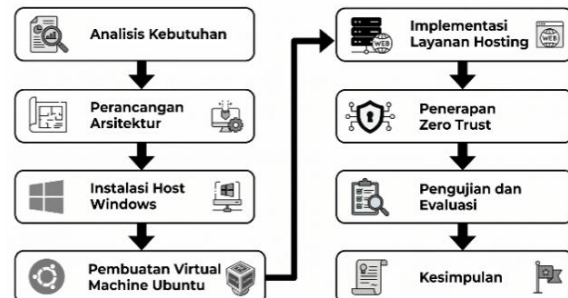
- Analisis kebutuhan**
Pada tahap ini dilakukan identifikasi kebutuhan perangkat keras, perangkat lunak, layanan hosting, kebutuhan konektivitas, dan kebutuhan keamanan. Analisis ini bertujuan untuk memastikan bahwa lingkungan sistem yang dibangun sesuai dengan tujuan penelitian.
- Perancangan arsitektur sistem**
Setelah kebutuhan sistem diperoleh, tahap berikutnya adalah membuat rancangan arsitektur yang menggambarkan hubungan antara sistem operasi host Windows, aplikasi virtualisasi, mesin virtual Ubuntu, layanan hosting, dan mekanisme keamanan Zero Trust.
- Pembuatan lingkungan virtual**
Pada tahap ini dilakukan instalasi aplikasi virtualisasi pada Windows, kemudian dibuat sebuah virtual machine yang menjalankan Ubuntu. Mesin virtual tersebut dikonfigurasi dari sisi

sumber daya, jaringan, dan penyimpanan agar dapat digunakan sebagai server virtual.

- Implementasi layanan hosting**
Setelah Ubuntu berjalan dengan baik, dilakukan instalasi dan konfigurasi layanan hosting sesuai kebutuhan penelitian. Tahap ini bertujuan agar server virtual dapat digunakan untuk menyediakan layanan yang dapat diakses oleh pengguna.
- Penerapan keamanan Zero Trust**
Pada tahap ini diterapkan pengaturan keamanan yang menekankan verifikasi identitas, pembatasan hak akses, kontrol koneksi, dan pengawasan akses layanan. Pendekatan ini dilakukan agar tidak ada akses yang langsung dipercaya tanpa proses verifikasi.
- Pengujian sistem**
Pengujian dilakukan terhadap fungsi sistem, kestabilan layanan, konektivitas jaringan, dan efektivitas pembatasan akses. Pengujian ini bertujuan untuk mengetahui apakah sistem telah berjalan sesuai rancangan.
- Evaluasi hasil**
Tahap akhir adalah menganalisis hasil pengujian untuk menilai efektivitas sistem dalam menyediakan layanan hosting yang efisien, fleksibel, dan aman.

3.3. Diagram Alur Metode Penelitian

Diagram alur metode penelitian dapat disajikan dalam bentuk teks sebagai berikut:



Gambar 1. Alur Penelitian

3.4. Implementasi Virtual Machine

Implementasi virtual machine dalam penelitian ini dilakukan dengan menggunakan sistem operasi Windows sebagai host operating system dan Ubuntu sebagai guest operating system. Ubuntu dipilih karena memiliki stabilitas yang baik, kebutuhan sumber daya yang relatif efisien, serta dukungan luas untuk implementasi layanan server dan administrasi jaringan. Melalui virtualisasi ini, server dapat dijalankan secara terisolasi dari sistem host, sehingga risiko gangguan terhadap sistem utama dapat dikurangi.

Selain itu, penggunaan virtual machine juga memudahkan proses konfigurasi, pengujian, dan pemeliharaan layanan. Jika terjadi kesalahan konfigurasi atau gangguan pada server virtual, sistem host tetap dapat berjalan secara normal. Hal ini

menjadikan virtualisasi sebagai pendekatan yang sesuai untuk pengembangan infrastruktur hosting yang fleksibel dan hemat biaya.

3.5. Penerapan Model Keamanan Zero Trust

Model keamanan Zero Trust diterapkan dengan asumsi bahwa tidak ada entitas, baik pengguna, perangkat, maupun koneksi, yang secara otomatis dapat dipercaya. Setiap akses ke server virtual Ubuntu harus melalui proses verifikasi identitas dan pemeriksaan hak akses. Dengan pendekatan ini, sistem dapat meminimalkan risiko penyusupan, akses ilegal, dan penyalahgunaan layanan.

Penerapan model ini dilakukan melalui pembatasan akses terhadap layanan yang terbuka, pengaturan akun pengguna, pembatasan port atau koneksi tertentu, serta pemantauan terhadap aktivitas akses. Prinsip ini mendukung keamanan sistem hosting karena server tidak hanya dilindungi dari sisi jaringan luar, tetapi juga dari kemungkinan akses tidak sah yang berasal dari lingkungan internal.

3.6. Teknik Pengujian

Pengujian sistem dalam penelitian ini dilakukan dengan beberapa skenario, yaitu:

- Pengujian fungsional, untuk memastikan virtual machine Ubuntu dapat berjalan di atas Windows dan layanan hosting dapat beroperasi dengan baik.
- Pengujian konektivitas, untuk memastikan server virtual dapat diakses melalui jaringan sesuai konfigurasi.
- Pengujian keamanan dasar, untuk memastikan mekanisme Zero Trust dapat membatasi akses hanya kepada pengguna atau perangkat yang berwenang.
- Pengujian isolasi sistem, untuk memastikan lingkungan virtual Ubuntu berjalan terpisah dari sistem host Windows.

3.7. Teknik Analisis Data

Data yang diperoleh dari hasil pengujian dianalisis menggunakan pendekatan deskriptif. Analisis dilakukan dengan membandingkan hasil implementasi sistem terhadap tujuan penelitian, yaitu efisiensi infrastruktur, fleksibilitas pengelolaan layanan, dan peningkatan keamanan akses. Hasil analisis kemudian digunakan sebagai dasar dalam menarik kesimpulan mengenai kelayakan sistem yang dikembangkan.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Implementasi Sistem

Penelitian ini menghasilkan sebuah infrastruktur hosting mobile berbasis microserver dengan memanfaatkan teknologi virtual machine dan model keamanan Zero Trust. Implementasi sistem dilakukan menggunakan sistem operasi Windows sebagai host operating system dan Ubuntu sebagai guest operating system yang dijalankan melalui aplikasi virtualisasi.

Pada lingkungan virtual Ubuntu dilakukan instalasi dan konfigurasi layanan hosting, sehingga Ubuntu berperan sebagai server virtual utama.

Hasil implementasi menunjukkan bahwa virtual machine Ubuntu berhasil dijalankan dengan baik di atas sistem operasi Windows. Alokasi sumber daya seperti prosesor, RAM, dan penyimpanan virtual dapat dilakukan sesuai kebutuhan sistem. Setelah mesin virtual aktif, layanan hosting dapat diinstal dan dijalankan secara normal. Hal ini menunjukkan bahwa pendekatan virtualisasi mampu membangun lingkungan server yang fleksibel tanpa harus menggunakan server fisik terpisah.

Selain dari sisi fungsional, penelitian ini juga berhasil menerapkan model keamanan Zero Trust pada sistem yang dibangun. Penerapan dilakukan melalui pembatasan akses pengguna, verifikasi identitas, dan pengaturan hak akses terhadap layanan tertentu. Dengan demikian, sistem tidak memberikan kepercayaan otomatis kepada setiap pengguna atau perangkat yang terhubung, melainkan menerapkan prinsip never trust, always verify.

Untuk mengetahui kinerja sistem, dilakukan pengukuran terhadap beberapa parameter, yaitu penggunaan CPU, penggunaan memori, waktu respons akses layanan, dan tingkat keberhasilan akses. Selain itu, dilakukan juga pengujian keamanan dasar untuk melihat efektivitas pembatasan akses berbasis Zero Trust.

4.2. Hasil Pengujian Fungsional

Pengujian fungsional dilakukan untuk memastikan bahwa seluruh komponen sistem berjalan sesuai rancangan. Hasil pengujian fungsional ditunjukkan pada Tabel 1.

Tabel 1. Hasil Pengujian

No	Komponen yang Diuji	Skenario Pengujian	Hasil
1	Host Windows	Sistem operasi host berjalan normal	Berhasil
2	Virtual Machine Ubuntu	Ubuntu dapat dijalankan pada Windows	Berhasil
3	Konfigurasi jaringan VM	VM memperoleh koneksi jaringan	Berhasil
4	Layanan hosting	Layanan dapat dijalankan pada Ubuntu	Berhasil
5	Akses pengguna	Pengguna dapat mengakses layanan sesuai hak akses	Berhasil
6	Pembatasan akses	Pengguna tanpa otorisasi ditolak	Berhasil

Berdasarkan Tabel 1, seluruh komponen utama dapat berjalan sesuai fungsi yang direncanakan. Hasil ini menunjukkan bahwa integrasi antara host Windows, mesin virtual Ubuntu, layanan hosting, dan mekanisme keamanan dapat diimplementasikan dengan baik.

4.3. Hasil Pengukuran Kinerja Sistem

Pengukuran dilakukan sebanyak 10 kali percobaan untuk memperoleh gambaran kinerja sistem. Parameter yang diamati meliputi penggunaan CPU, penggunaan RAM, dan waktu respons akses layanan.

Tabel 2. Hasil Pengukuran Kerja

Percobaan	CPU (%)	RAM (MB)	Response Time (ms)	Status Akses
1	24	1180	210	Berhasil
2	27	1215	225	Berhasil
3	25	1198	218	Berhasil
4	29	1240	235	Berhasil
5	26	1204	220	Berhasil
6	30	1268	240	Berhasil
7	28	1231	230	Berhasil
8	24	1175	212	Berhasil
9	31	1280	245	Berhasil
10	27	1220	228	Berhasil

Berdasarkan Tabel 2, terlihat bahwa penggunaan CPU berada pada rentang 24% hingga 31%, sedangkan penggunaan memori berada pada rentang 1175 MB hingga 1280 MB. Waktu respons layanan berkisar antara 210 ms hingga 245 ms. Secara umum, hasil ini menunjukkan bahwa sistem mampu berjalan dengan stabil pada beban pengujian dasar.

4.4. Perhitungan Nilai Rata-Rata

Untuk mengetahui performa umum sistem, dilakukan perhitungan rata-rata pada setiap parameter menggunakan rumus:

$$\bar{x} = \frac{\sum x}{n} \quad (1)$$

Dengan:

$\bar{x}$ = nilai rata – rata

$\sum x$ = jumlah seluruh data

n = jumlah Percobaan

Adapun hasil dari pengukuran didapatkan hasil pada Tabel 3.

Tabel 3. Hasil Rata-Rata Pengujian

Komponen	Percobaan	Hasil
CPU	10	27.1%
RAM	10	1221.1 MB
Response Time	10	226.3ms

4.5. Perhitungan Nilai Rata-Rata

Pengujian keamanan dilakukan untuk melihat apakah mekanisme pembatasan akses berjalan sesuai prinsip Zero Trust. Pengujian dilakukan pada beberapa skenario, seperti akses pengguna terdaftar, akses pengguna tidak terdaftar, dan percobaan akses ke layanan tanpa izin.

Tabel 4. Perhitungan Nilai Rata-Rata

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual
1	Pengguna valid login ke sistem	Diterima	Sesuai
2	Pengguna tidak valid mencoba login	Ditolak	Sesuai
3	Pengguna tanpa hak akses membuka layanan tertentu	Ditolak	Sesuai
4	Pengguna valid mengakses layanan sesuai izin	Diterima	Sesuai
5	Percobaan koneksi dari perangkat tidak dikenal	Diverifikasi/ditolak	Sesuai

Berdasarkan Tabel 4, mekanisme keamanan Zero Trust mampu menjalankan fungsi dasar verifikasi dan pembatasan akses. Hal ini membuktikan bahwa sistem tidak hanya berjalan secara fungsional, tetapi juga memiliki lapisan keamanan yang lebih baik dibandingkan sistem yang langsung mempercayai seluruh entitas dalam jaringan.

4.6. Pembahasan

Hasil penelitian menunjukkan bahwa penggunaan Ubuntu sebagai virtual machine di atas Windows mampu menyediakan lingkungan server yang cukup stabil untuk mendukung layanan hosting mobile. Virtualisasi memberikan fleksibilitas karena layanan server dapat dijalankan secara terisolasi dari sistem host. Kondisi ini penting karena jika terjadi kesalahan konfigurasi pada server virtual, sistem host tetap dapat berjalan normal.

Dari sisi kinerja, nilai rata-rata penggunaan CPU sebesar 27,1% dan penggunaan RAM sebesar 1221,1 MB menunjukkan bahwa sistem belum membebani sumber daya secara berlebihan. Waktu respons rata-rata sebesar 226,3 ms juga menunjukkan bahwa layanan masih cukup responsif untuk penggunaan dasar. Hasil ini mendukung bahwa pendekatan microserver dan virtualisasi cocok digunakan untuk kebutuhan hosting skala kecil hingga menengah.

Penerapan model keamanan Zero Trust juga memberikan hasil yang baik. Semua skenario pengujian keamanan dasar menunjukkan hasil sesuai harapan, terutama dalam hal penolakan akses terhadap pengguna atau perangkat yang tidak memiliki izin. Dengan demikian, sistem yang dikembangkan tidak hanya efisien dari sisi infrastruktur, tetapi juga memiliki penguatan keamanan akses.

Jika dibandingkan dengan pendekatan server konvensional, model yang dibangun dalam penelitian ini memiliki beberapa keunggulan. Pertama, dari sisi efisiensi, sistem dapat dibangun tanpa memerlukan server fisik besar. Kedua, dari sisi fleksibilitas, layanan

dapat dikelola melalui mesin virtual yang mudah dikonfigurasi. Ketiga, dari sisi keamanan, pendekatan Zero Trust memberikan perlindungan tambahan melalui mekanisme verifikasi akses yang berkelanjutan.

Namun demikian, penelitian ini masih memiliki keterbatasan. Pengujian yang dilakukan masih berada pada skala dasar dan belum mencakup uji beban tinggi, simulasi serangan siber yang kompleks, maupun analisis performa jangka panjang. Oleh karena itu, penelitian selanjutnya dapat diarahkan pada pengujian stress test, analisis skalabilitas, dan evaluasi keamanan yang lebih mendalam.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa pengembangan infrastruktur hosting mobile menggunakan microserver berbasis virtual machine dengan penerapan model keamanan Zero Trust berhasil diimplementasikan dengan baik. Sistem dibangun menggunakan Windows sebagai host operating system dan Ubuntu sebagai guest operating system yang dijalankan melalui teknologi virtualisasi. Hasil implementasi menunjukkan bahwa mesin virtual Ubuntu mampu berfungsi sebagai server untuk menjalankan layanan hosting secara stabil, fleksibel, dan terisolasi dari sistem host.

Hasil pengujian menunjukkan bahwa seluruh komponen utama sistem, mulai dari host, mesin virtual, layanan hosting, hingga mekanisme kontrol akses, dapat berjalan sesuai rancangan. Berdasarkan data pengukuran, sistem memiliki rata-rata penggunaan CPU sebesar 27,1%, rata-rata penggunaan RAM sebesar 1221,1 MB, dan rata-rata response time sebesar 226,3 ms. Selain itu, tingkat keberhasilan akses layanan mencapai 100% pada pengujian dasar. Hasil ini menunjukkan bahwa sistem yang dikembangkan cukup layak untuk mendukung kebutuhan hosting mobile skala kecil hingga menengah.

Berdasarkan hasil penelitian yang telah dilakukan, pengembangan sistem hosting mobile berbasis microserver dengan penerapan virtual machine dan model keamanan Zero Trust masih dapat ditingkatkan pada penelitian selanjutnya. Disarankan untuk melakukan pengujian dengan skala yang lebih besar, seperti stress testing, pengujian multi-user, serta analisis performa dan kestabilan sistem dalam jangka waktu operasional yang lebih panjang.

Selain itu, implementasi keamanan Zero Trust dapat dikembangkan lebih lanjut melalui penambahan fitur keamanan seperti multi-factor authentication (MFA), pemantauan log secara real-time, sistem deteksi intrusi, serta segmentasi jaringan yang lebih detail untuk meningkatkan perlindungan akses terhadap sistem. Pengembangan tersebut diharapkan mampu menghasilkan infrastruktur hosting yang lebih optimal, aman, fleksibel, dan siap diterapkan pada lingkungan operasional nyata dengan kebutuhan layanan digital yang lebih kompleks.

DAFTAR PUSTAKA

- [1] Fikri, M. S., & Tedyyana, A. (2026). Rancang Bangun Sistem Hosting Mandiri Dengan Raspberry Pi Dan Aapanel Sebagai Solusi Alternatif Web Hosting Murah. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 10(2), 2329-2335
- [2] Editya, A. S., Lega, C., & Ussada, U. (2022). Kinerja Microserver untuk Menangani Lalu Lintas Berat di Host Server Khusus untuk Jaringan Area Lokal. *SUBMIT: Jurnal Ilmiah Teknologi Infomasi dan Sains*, 2(1), 17-21.
- [3] Editya, A. S., & Kurniati, N. (2020, December). Microserver Performance to Handle Heavy Traffic in Dedicated Server Host for Local Area Network. In *2020 IEEE International Conference on Communication, Networks and Satellite (Commnetsat)* (pp. 170-173). IEEE.
- [4] Goldberg, R. P. (1973, March). Architecture of virtual machines. In *Proceedings of the workshop on virtual computer systems* (pp. 74-112)
- [5] Chandra, R., & Sitorus, A. T. (2024). Virtualisasi Server Menggunakan Proxmox Untuk Mengoptimalkan Resource Server Pada SMK Bhakti Persada. *Jurnal Multidisiplin Ilmu Akademik*, 1(2), 69-80.
- [6] Gian Raihan Firdaus, F. (2025). Perancangan Prototype Infrastruktur Cloud Dengan Proxmox Hypervisor Untuk Mendukung Layanan Digital Dpmpstsp Garut (Doctoral dissertation, institut pendidikan indonesia).
- [7] Alamin, Z., & Mu'min, M. A. (2025). Analisis keamanan jaringan pada sistem kendali jarak jauh untuk infrastruktur kritis. *Jurnal Pengembangan Sains dan Teknologi*, 1(1), 25-41.
- [8] Fauzi, Y., & Hamdan, R. A. (2025). Pendekatan Metodologis dalam Deteksi Ancaman Siber pada Server Hosting Menggunakan NMAP dan Metasploit. *sudo Jurnal Teknik Informatika*, 4(1), 1-10.
- [9] Rahman, R. R. R., Ilyas, M. F. I. F., & Syawal, M. S. (2025). Implementasi Zero Trust Arsitektur Pada Jaringan Hybrid Work. *Journal of System & Technology (SYSTEC)*, 1(1), 14-19.
- [10] Rahman, R. R. R., Ilyas, M. F. I. F., & Syawal, M. S. (2025). Implementasi Zero Trust Arsitektur Pada Jaringan Hybrid Work. *Journal of System & Technology (SYSTEC)*, 1(1), 14-19.
- [11] ALFARIZHI, R. A. (2024). *IMPLEMENTASI PROTOTYPE BISNIS IT LAYANAN VPS DAN WEB HOSTING SEBAGAI LABORATORIUM RESEARCH MAHASISWA UNIVERSITAS BINA DARMA* (Doctoral dissertation, Universitas Bina Darma).
- [12] Rojabi, M. A. (2025). *Mengamankan Windows 11: Panduan Enkripsi dan Zero Trust*. Afdan Rojabi Publisher.
- [13] Nazzarina, F. K. (2025). Analisis Keamanan Siber pada Platform Digital Pemerintahan

- Modern. *Jurnal Teknologi Komputer Modern*, 1(1), 1-8.
- [14] Okpatrioka, O. (2023). Research and development (R&D) penelitian yang inovatif dalam pendidikan. *Dharma Acariya Nusantara: Jurnal Pendidikan, Bahasa dan Budaya*, 1(1), 86-100.
- [15] Sinaga, A., Sinaga, A. M., & Sianturi, R. A. (2023). DESAIN ARSITEKTUR VIRTUALISASI PENGEMBANGAN SISTEM INFORMASI MANAJEMEN PENGELOLAAN SAMPAH RUMAH TANGGA PADA BANK SAMPAH BERBASIS CONTAINER DOCKER. *Sebatik*, 27(2), 560-569.