Implementasi Konsep *Zero Trust Architecture* pada *Cloud Environment* Menggunakan *Microsoft Azure*

Vincencius Galvin Hermanto[1)], Edwin Lesmana Tjiong[2)]

Informatika, Fakultas Ilmu Komputer dan Desain, Universitas Kalbis
Jalan Pulomas Selatan Kav. 22, Jakarta 13210
[1)] *Email: Vincencius.galvin@gmail.com*
[2)] *Email: Edwin.Tjiong@kalbis.ac.id*

Abstract: *In an era of rapid digital transformation, cybersecurity has become a top priority for organizations adopting cloud computing services. One increasingly adopted security approach is Zero Trust Architecture (ZTA), which follows the principle of "never trust, always verify." This research aims to implement Zero Trust Architecture in a cloud environment using Microsoft Azure to enhance infrastructure security posture. The study explores core components of ZTA—such as identity control, risk-based access policies, and continuous monitoring—and demonstrates how Azure services such as Azure Monitoring, Azure Identity and Access Management (IAM), Microsoft Defender for Cloud, Azure Policy, Azure Web Application Firewall (WAF), and Azure VPN can be utilized to build this architecture. The implementation results indicate that adopting ZTA in Azure provides more granular and adaptive security controls against modern cyber threats. This research is expected to serve as a technical reference for organizations seeking to strengthen their cloud infrastructure security through the Zero Trust approach.*
Keywords: *Cloud Infrastructure, Cloud Security, Microsoft Azure, Zero Trust Architecture.*

Abstrak: *Dalam era transformasi digital yang semakin pesat, keamanan siber menjadi prioritas utama bagi organisasi yang mengadopsi layanan cloud computing. Salah satu pendekatan keamanan yang semakin banyak diadopsi adalah Zero Trust Architecture (ZTA), yang mengusung prinsip "never trust, always verify". Penelitian ini bertujuan untuk mengimplementasikan arsitektur Zero Trust pada lingkungan cloud menggunakan Microsoft Azure guna meningkatkan postur keamanan infrastruktur. Studi ini mencakup identifikasi komponen utama ZTA, seperti kontrol identitas, kebijakan akses berbasis risiko, dan pemantauan berkelanjutan, serta bagaimana layanan Azure—seperti Azure Monitoring, Azure Identity and Access Management (IAM), Microsoft Defender for Cloud, Azure Policy, Azure Web Application Firewall (WAF), dan Azure VPN—dapat digunakan untuk membangun arsitektur tersebut. Hasil implementasi menunjukkan bahwa penerapan ZTA dalam Azure mampu memberikan kontrol keamanan yang lebih granular dan adaptif terhadap ancaman siber modern. Penelitian ini diharapkan dapat menjadi referensi teknis bagi organisasi yang ingin memperkuat keamanan infrastruktur cloud mereka melalui pendekatan Zero Trust.*
Kata Kunci: *Infrastruktur Cloud, Keamanan Cloud, Microsoft Azure, Zero Trust Architecture.*

I. PENDAHULUAN

Perkembangan teknologi digital telah mendorong perusahaan untuk melakukan digitalisasi dalam proses bisnisnya. Salah satu teknologi yang mendukung transformasi ini adalah cloud computing, yang ditawarkan oleh berbagai penyedia layanan seperti *Google Cloud Platform*, *Amazon Web Services*, dan *Microsoft Azure*. Konsep *cloud computing* sendiri berasal dari arsitektur perangkat lunak terdistribusi (*distributed software architecture*), yang bertujuan mempermudah pengguna dalam mengakses dan menggunakan sumber daya TI secara fleksibel, khususnya dalam

pengembangan perangkat lunak melalui cloud resources[1].

Cloud resources merupakan sumber daya TI yang dapat diakses melalui jaringan internet dan umumnya disediakan dalam bentuk layanan berbayar oleh penyedia layanan cloud [2]. Model layanan yang ditawarkan mencakup *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), *Container as a Service* (CaaS), dan *Software as a Service* (SaaS) [1]. Layanan ini memberikan kemudahan dalam proses pengumpulan, pemrosesan, dan penyimpanan data secara daring [2].

Namun, meningkatnya penggunaan *cloud computing* juga memunculkan tantangan baru, khususnya dalam hal keamanan. Lingkungan *cloud* yang berbasis protokol internet standar dan virtualisasi menjadikannya rentan terhadap serangan siber [3]. Teknologi virtualisasi memungkinkan penciptaan perangkat keras, sistem operasi, dan jaringan secara virtual dengan keunggulan pada skalabilitas dan kecepatan [4]. Oleh karena itu, keamanan menjadi aspek krusial dalam membangun arsitektur *cloud* yang sesuai dengan *security compliance* yang berlaku [1].

Berbagai pendekatan telah dikembangkan untuk memperkuat postur keamanan *cloud*, seperti *Network Intrusion Detection and Countermeasure Selection System* (NICE) dan *Autonomous Cloud Intrusion Response System* (ACIRS). Teknologi ACIRS diklaim lebih efektif dalam memitigasi risiko serangan pada jaringan virtual cloud [1]. Selain itu, kemajuan teknologi machine learning turut dimanfaatkan untuk mendeteksi ancaman secara otomatis dan memberikan peringatan kepada administrator sistem, serta mengevaluasi kondisi infrastruktur cloud secara berkala [3].

Salah satu pendekatan keamanan yang berkembang pesat adalah konsep *Zero Trust*. *Zero Trust* merupakan paradigma keamanan siber yang menekankan pada perlindungan sumber daya sistem dengan prinsip bahwa setiap permintaan akses harus divalidasi berdasarkan identitas dan konteks, serta dibatasi sesuai kebutuhan [5]. Konsep ini tidak hanya menangani ancaman eksternal, tetapi juga dirancang untuk mengurangi risiko dari dalam, termasuk akibat kesalahan manusia—yang menjadi salah satu faktor utama pelanggaran keamanan sistem [6].

Salah satu prinsip kunci dari *Zero Trust* adalah *principle of least privilege*, yaitu membatasi hak akses setiap pengguna (baik internal maupun eksternal) secara granular sesuai kebutuhan [5]. *Zero Trust* juga memperhatikan keamanan komunikasi internal, kebijakan akses dinamis, serta pemantauan kondisi integritas sistem secara rutin [5].

Penerapan *Zero Trust Architecture* terbukti mampu mengatasi berbagai permasalahan keamanan dalam lingkungan *cloud*, seperti *unauthorized access* dan *unaudited access list*. Misalnya, penerapan kebijakan berbasis waktu dapat mencegah akses sistem di luar jadwal yang telah ditentukan, sementara automasi audit dan pemutusan akses dapat menghindari penyalahgunaan oleh mantan karyawan. Dengan demikian, kontrol akses dapat diatur secara ketat berdasarkan identitas, waktu, dan konteks penggunaan.

Penelitian ini bertujuan untuk menerapkan *Zero Trust Architecture* pada lingkungan cloud computing menggunakan *Microsoft Azure*. Pendekatan ini diharapkan dapat membentuk arsitektur keamanan cloud yang lebih adaptif, presisi, dan sesuai dengan tantangan keamanan sistem informasi modern.

II. METODE PENELITIAN

Penelitian ini dilakukan melalui pendekatan *literature review* terhadap karya-karya ilmiah yang relevan, guna memperoleh pemahaman mendalam

mengenai penerapan *Zero Trust Architecture (ZTA)* pada lingkungan *cloud computing*. Tinjauan pustaka digunakan untuk mengidentifikasi kelebihan dan kekurangan pendekatan yang telah dilakukan oleh peneliti sebelumnya, serta merumuskan fondasi teori yang menjadi dasar dalam penelitian ini.

Peninjauan pertama merujuk pada jurnal yang ditulis oleh Sina Ahmadi (2024) [7], yang membahas implementasi *ZTA* pada arsitektur *cloud*, mencakup tantangan, peluang, serta dampak positif penerapannya. Jurnal ini menyatakan bahwa *ZTA* memperkuat keamanan sistem secara signifikan dibandingkan pendekatan tradisional, karena kebijakan zero trust menuntut autentikasi yang lebih ketat untuk melindungi informasi sensitif dalam sistem [7]. Implementasi *ZTA* mencakup pengelolaan akses pengguna terhadap *cloud resources*, perlindungan terhadap jalur akses jaringan, serta segmentasi yang mendalam dalam sistem. Seperti dijelaskan pada bab sebelumnya, faktor internal merupakan penyumbang utama pelanggaran keamanan karena manusia merupakan *weakest link* dalam suatu infrastruktur. Model keamanan *zero trust* dapat memitigasi hal ini karena prinsip dasarnya menganggap bahwa tidak ada entitas yang dapat dipercaya sepenuhnya dalam sistem, sehingga setiap aktivitas pengguna harus dipantau dan divalidasi [7].

Jurnal tersebut juga menyoroti peluang masa depan dari implementasi *ZTA* yang semakin luas, seiring perkembangan teknologi *cloud* dan kemajuan di bidang *machine learning (ML)* serta *artificial intelligence (AI)* yang dapat memperkuat sistem deteksi ancaman secara *real-time* [7]. Ke depan, *ZTA* diproyeksikan akan terintegrasi secara lebih erat dengan sistem keamanan berbasis pengguna (*user-centric security*).

Peninjauan kedua mengacu pada artikel ilmiah oleh Himanshu Sharma (2022) [8], yang membahas implementasi *ZTA* dalam konteks *cloud* serta evolusi model keamanan dari sistem tradisional menuju paradigma *zero trust*. Artikel ini menunjukkan bahwa sistem keamanan saat ini berkembang dari model *perimeter-based security*, yang berasumsi bahwa ancaman berasal dari luar sistem [8]. Sebaliknya, *ZTA* memberikan akses berdasarkan kebijakan dinamis dan mempertahankan validitas akses secara berkelanjutan.

Dalam penerapannya, *ZTA* memerlukan beberapa komponen penting, seperti penggunaan *Identity and Access Management (IAM)* dengan otentikasi multifaktor, segmentasi jaringan melalui *virtual private network (VPN)*, serta integrasi sistem keamanan dengan *Security Information and Event Management (SIEM)* sebagai alat pemantauan sistem [8].

Kedua tinjauan pustaka tersebut membahas implementasi *ZTA* dalam arsitektur *cloud*. Namun, berbeda dengan pendekatan analitis dari kedua penelitian tersebut, penelitian ini difokuskan pada pembuktian langsung implementasi *ZTA* dengan menggunakan platform *Microsoft Azure*. Pendekatan ini bertujuan untuk mengkaji efektivitas konsep *zero trust* terhadap insiden seperti *unauthorized access* dan *unaudited access list*, serta mengevaluasi bagaimana *ZTA* dapat diintegrasikan dalam arsitektur *cloud* secara praktis dan terukur. Pemilihan *Microsoft Azure* didasarkan pada posisinya sebagai salah satu dari tiga penyedia layanan *cloud* terkemuka [2], serta ketersediaan fitur keamanannya seperti *Microsoft Defender for Cloud* dan dukungannya terhadap model *hybrid cloud* [9][10].

A. *Zero Trust Architecture*

Zero Trust Architecture atau disingkat *ZTA*, merupakan salah satu *framework* yang menjadi standar dalam membangun sistem yang aman. Secara konseptual, *ZTA* telah dikenal jauh sebelum penggunaannya secara luas di

bidang keamanan sistem, melalui strategi yang dikenal sebagai *Black Core (BCORE)*[5]. Inti dari strategi ini adalah keamanan yang berfokus pada setiap *transaction* atau *event* yang terjadi di dalam sistem.

Menurut definisi resmi dari *National Institute of Standards and Technology (NIST)*, *ZTA* adalah paradigma keamanan siber yang menekankan proteksi terhadap setiap komponen dalam sistem, dengan premis bahwa setiap akses yang diberikan harus terus dievaluasi secara berkelanjutan [5]. Kerangka ini mencakup semua komponen sistem, koneksi antar komponen, serta seluruh pengguna—baik yang mengakses secara lokal maupun *remote*.

ZTA bertujuan untuk meminimalkan *attack surface* dari sistem dengan pendekatan berbasis hubungan antar komponen, perencanaan alur sistem, dan kebijakan akses yang dinamis [5].

1. Prinsip Zero Trust Architecture

Dalam penerapannya, infrastruktur yang mengadopsi *ZTA* harus mematuhi prinsip-prinsip berikut [5]:

- Seluruh *data sources* dan *computing services* dianggap sebagai bagian dari sistem yang wajib dilindungi.
- Semua komunikasi antar komponen harus dilakukan secara aman (*secure communication*), tanpa bergantung pada lokasi komponen.
- Akses diberikan dengan batasan waktu tertentu (*time-limited access*) dan hanya sesuai kebutuhan.
- Akses ditentukan oleh kebijakan yang bersifat dinamis (*dynamic access policy*), menyesuaikan dengan *best practice* keamanan siber.
- Komponen sistem harus dipantau dan dievaluasi keamanannya secara rutin (*continuous system monitoring*).
- Seluruh permintaan akses harus dievaluasi sebelum diberikan otorisasi (*evaluated access*).
- Semua informasi dari komponen, jaringan, dan aktivitas akses harus dikumpulkan dan dianalisis untuk peningkatan postur keamanan (*system log analysis*).

B. Cloud Computing

Cloud computing merupakan tonggak penting dalam evolusi teknologi informasi yang menekankan prinsip *on-demand accessibility* terhadap layanan dan produk komputasi. Teknologi ini mengintegrasikan konsep-konsep seperti *virtualization*, *distributed computing*, *networking*, dan *software services* ke dalam satu platform yang memiliki tingkat aksesibilitas dan skalabilitas tinggi [11].

Dengan dukungan pendekatan *service-oriented architecture (SOA)*, *cloud computing* memungkinkan pengguna mengonfigurasi dan menggunakan layanan komputasi sesuai kebutuhan, baik dari sisi fungsi, skala, maupun spesifikasi teknis [11].

Salah satu pilar utama dalam *cloud computing* adalah *virtualization*, yaitu teknologi yang mengabstraksi fungsionalitas perangkat keras dan perangkat lunak, sehingga memungkinkan fleksibilitas dan isolasi sistem yang lebih baik. *Virtualization* juga memungkinkan portabilitas dan modifikasi sistem secara cepat, efisien, dan skalabel [4].

Model Layanan Cloud Computing

Dalam praktiknya, *cloud computing* menawarkan tiga model layanan utama [4]:

- **Private Cloud**
  Model layanan yang digunakan secara eksklusif oleh suatu organisasi, dengan akses terbatas hanya bagi pengguna internal.

- **Public Cloud**

Layanan yang tersedia secara umum melalui internet, menggunakan model pembayaran *pay-per-use*, dan cocok untuk pengguna individu maupun bisnis.

- **Hybrid Cloud**
  Gabungan antara *private* dan *public cloud* yang menggabungkan keunggulan keduanya, memungkinkan organisasi mengelola layanan internal secara privat dan layanan publik untuk kebutuhan eksternal [10].

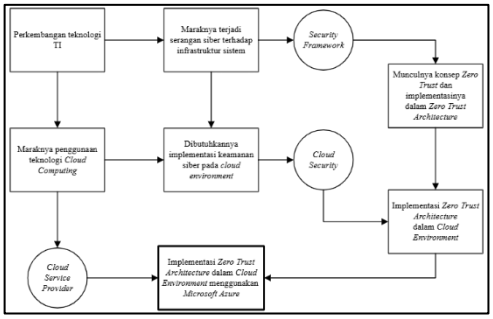
C. Microsoft Azure

Untuk mengakses layanan *cloud computing*, pengguna memanfaatkan layanan dari penyedia pihak ketiga yang dikenal sebagai *cloud service providers*. Penyedia ini menawarkan berbagai jenis layanan berbasis *cloud*, mulai dari *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)*, *Software as a Service (SaaS)*, hingga yang terbaru *Infrastructure as Code (IaC)* [2].

Salah satu penyedia utama dalam industri ini adalah *Microsoft Azure*. Sebagai produk dari Microsoft, *Azure* menawarkan berbagai layanan *cloud computing* dengan tingkat *availability* yang tinggi, serta mendukung integrasi *hybrid cloud*, keamanan melalui *Microsoft Defender for Cloud*, dan kompatibilitas dengan produk ekosistem Microsoft lainnya [9][10].

Penelitian ini menggunakan *Microsoft Azure* sebagai platform untuk mengimplementasikan *Zero Trust Architecture*. Pemilihan ini didasarkan pada kelengkapan fitur keamanan yang dimiliki oleh *Azure*, serta posisinya sebagai salah satu dari tiga penyedia layanan *cloud* terkemuka bersama *Amazon Web Services (AWS)* dan *Google Cloud Platform (GCP)* [2]. Implementasi juga akan difokuskan pada pemanfaatan model *hybrid cloud* serta penerapan fitur keamanan berbasis identitas dan kebijakan akses yang ditawarkan oleh platform tersebut.

D. Kerangka Pemikiran



Gambar 1 Kerangka Pemikiran

Kerangka pemikiran dalam penelitian ini dibangun atas dasar perkembangan *teknologi informasi* yang telah menjadi standar industri saat ini. Salah satu perkembangan utama adalah *cloud computing*, yang menjadi fokus kajian dalam penelitian ini. Seiring dengan kemajuan teknologi, ancaman serangan siber terhadap infrastruktur sistem juga semakin meningkat, sehingga memicu tingginya permintaan terhadap penerapan keamanan siber pada lingkungan *cloud*. Hal ini melatarbelakangi kemunculan sektor *cloud security* sebagai bagian integral dari sistem pertahanan digital modern.

Sebagai respons terhadap tantangan tersebut, beberapa standar keamanan telah dikembangkan dalam bentuk *security frameworks*, salah satunya adalah konsep *Zero Trust Architecture (ZTA)*. Penelitian ini berfokus pada implementasi *ZTA* dalam lingkungan *cloud* menggunakan *Microsoft Azure* sebagai salah satu *cloud service provider* yang banyak digunakan di industri. Tujuan utama dari penelitian ini adalah untuk menyediakan kerangka implementasi *ZTA* yang terukur dan aplikatif dalam konteks keamanan sistem berbasis *cloud*, khususnya melalui pemanfaatan fitur dan layanan yang tersedia pada platform *Microsoft Azure*.

E. Prosedur Penelitian

1. Pembuatan Infrastruktur Sistem

Untuk mendemonstrasikan penerapan *Zero Trust Architecture (ZTA)* dalam lingkungan *cloud* menggunakan *Microsoft Azure*, dua infrastruktur *cloud* yang berbeda dirancang. Tujuan pendekatan ini adalah memberikan perspektif komparatif terhadap efektivitas implementasi *ZTA*. Infrastruktur pertama, disebut *Project-Default*, dibangun tanpa mengadopsi prinsip-prinsip *ZTA*. Sedangkan infrastruktur kedua, *Project-ZTA*, secara eksplisit menerapkan konsep *ZTA* ke dalam seluruh komponennya.

2. Perbandingan antara Implementasi ZTA Menggunakan Panduan *Azure* dengan Penelitian Ini

Setelah kedua infrastruktur selesai dibangun, dilakukan pengujian terhadap masing-masing komponen untuk mencerminkan sejauh mana fungsionalitasnya mendukung tujuh prinsip dasar *ZTA* sebagaimana dijelaskan oleh *National Institute of Standards and Technology (NIST)*. Selain itu, dilakukan pula perbandingan antara desain *ZTA* yang diterapkan dalam penelitian ini dengan desain referensi dari *Microsoft* berdasarkan komponen dan estimasi biaya. Adapun komponen yang direkomendasikan oleh *Microsoft* untuk penerapan *ZTA* dalam platform *Azure* antara lain adalah sebagai berikut [12]:

- ***Azure Key Vault*** – Layanan untuk menyimpan dan mengelola *secrets*, *keys*, serta *certificates* secara aman, guna melindungi data sensitif dari akses tidak sah.
- ***Azure Bastion*** – Layanan akses jarak jauh ke *virtual machine (VM)* tanpa perlu membuka IP publik.
- ***Just-in-Time Access*** – Memberikan akses terbatas waktu kepada pengguna terhadap *resources* tertentu.
- ***Azure Firewall*** – *Firewall* jaringan berbasis *cloud* dengan kontrol lalu lintas tingkat *layer 3–7* dan kemampuan *logging*.
- ***Azure DDoS Protection*** – Perlindungan terhadap serangan *Distributed Denial of Service*.
- ***Azure Active Directory (AD)*** – Layanan manajemen identitas yang mendukung *Single Sign-On (SSO)* dan *Multi-Factor Authentication (MFA)*.
- ***Azure Purview*** – Layanan *data governance* untuk pelacakan dan pengamanan aset data.
- ***Application Gateway*** – *Load balancer* dengan fitur *Web Application Firewall (WAF)*.
- ***Virtual Network Gateway*** – Penghubung jaringan antara *Azure* dan lingkungan *on-premises*.
- ***Azure Monitor*** – Platform pemantauan sistem dan aplikasi secara *real-time*.
- ***Azure Advisor*** – Alat rekomendasi berbasis *AI* untuk efisiensi biaya dan peningkatan keamanan.

3. Pengujian Implementasi Prinsip *Zero Trust*

Pengujian dilakukan pada masing-masing infrastruktur dengan skenario yang dirancang untuk menguji penerapan tujuh prinsip dasar *ZTA*:

- **Resources Include All Data and Services**
  Pengujian difokuskan pada pengaturan *granular access control* untuk setiap *resource* dalam satu *subscription*. Tidak ada pewarisan hak akses antar *resource*, sehingga setiap entitas harus memiliki izin eksplisit.

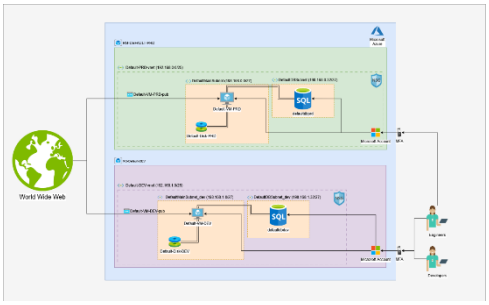
- **Secure-Line Communication**
  Semua komunikasi *inbound* dan *outbound* diarahkan melalui *Application Gateway* dan *VPN Gateway*, dengan penerapan enkripsi

dan penghapusan IP publik pada *resource* utama.

- **Time-Limited Access** Pengguna diberikan akses dengan batasan waktu melalui *time-based access policy*. Akses ini akan dicabut secara otomatis setelah waktu yang ditentukan.
- **Dynamic Access Policy** Setiap akses pengguna harus melalui proses *Multi-Factor Authentication (MFA)* sebagai bagian dari kebijakan akses dinamis.
- **Continuous System Monitoring** Aktivasi *resource health monitoring* memungkinkan pemantauan status sistem secara berkelanjutan untuk deteksi anomali sejak dini.
- **Evaluated Access** Permintaan akses dievaluasi berdasarkan prinsip *least privilege*, di mana akses hanya diberikan sesuai kebutuhan dan peran pengguna.
- **System Log Analysis** Seluruh aktivitas sistem dicatat melalui *activity logs* dan *diagnostic logs*. *Alert rules* diaktifkan untuk memberikan notifikasi saat terjadi aktivitas tidak biasa.

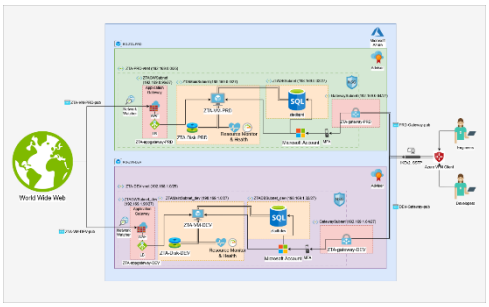
4. Perancangan Arsitektur Sistem

Sebelum implementasi, dilakukan perancangan arsitektur sistem yang mencakup perhitungan *Classless Inter-Domain Routing (CIDR)* untuk *virtual network* yang akan digunakan. Setiap komponen pada lingkungan *cloud* memerlukan alokasi *IP range* spesifik untuk mendukung fungsionalitasnya. Oleh karena itu, perencanaan *CIDR* menjadi tahap krusial dalam mendefinisikan skema jaringan yang efisien dan aman, dengan mempertimbangkan kebutuhan minimal *IP range* dari setiap layanan yang digunakan dalam infrastruktur.



Gambar 2 *Project-Default*

Diagram pada bagian atas menggambarkan struktur *Project-Default*, yaitu infrastruktur dasar sebelum penerapan konsep *Zero Trust Architecture (ZTA)*. Infrastruktur ini dibangun secara sederhana dengan hanya menggunakan beberapa *resources* utama seperti *Virtual Machine (VM)* dan *Database (DB)* yang langsung terhubung ke internet melalui *public IP address*. Konfigurasi seperti ini bersifat rentan karena membuka akses langsung terhadap komponen inti tanpa lapisan proteksi tambahan, sehingga meningkatkan permukaan serangan (*attack surface*) dan berpotensi menyebabkan kebocoran atau penyalahgunaan data sensitif.



Gambar 3 *Project-ZTA*

Sebaliknya, diagram berikutnya menunjukkan desain *Project-ZTA*, yaitu infrastruktur yang telah menerapkan prinsip-prinsip *ZTA*. Dalam struktur ini, seluruh *resources* utama seperti *VM* dan *DB* tidak lagi memiliki *public IP*, melainkan hanya dapat diakses melalui *Application Gateway* yang dilengkapi dengan *Web Application Firewall (WAF)*

sebagai lapisan proteksi terhadap trafik berbahaya.

Untuk melakukan akses administratif seperti *SSH*, pengguna harus terlebih dahulu terkoneksi ke jaringan internal melalui *Virtual Private Network (VPN)*. Selain itu, infrastruktur ini juga telah menerapkan mekanisme pemantauan melalui *Azure Monitor* serta sistem notifikasi otomatis menggunakan *alerting rules*.

Penggunaan *Azure Advisor* diintegrasikan untuk memberikan rekomendasi berbasis praktik terbaik, sementara otorisasi akses dikelola dengan pendekatan *Role-Based Access Control (RBAC)* melalui layanan *Azure Identity and Access Management (IAM)*, guna memastikan akses yang diberikan sesuai dengan prinsip *least privilege*.

III. HASIL DAN PEMBAHASAN

A. Implementasi *Zero Trust Architecture*

Setelah implementasi *Zero Trust Architecture* dilakukan sesuai rancangan diagram, penelitian ini menunjukkan bagaimana pengaruh konsep keamanan tersebut dalam *cloud environment* di *Microsoft Azure*.

Implementasi dikatakan berhasil apabila seluruh prinsip *Zero Trust* dapat diterapkan. Salah satu prinsip utamanya adalah bahwa semua sumber data dan layanan komputasi diperlakukan sebagai satu kesatuan sistem yang harus dilindungi. Hal ini dicapai dengan konfigurasi khusus terhadap komponen yang ada maupun penambahan komponen baru. Komponen-komponen yang digunakan antara lain:

1. **Azure Advisor** Fitur ini memantau *security posture* layanan *cloud* yang digunakan. Dua prinsip *Zero Trust* yang dipenuhi adalah *"continuous system monitoring and evaluation"* dan *"system log analysis"*. *Azure Advisor* melakukan pemindaian otomatis setiap 24 jam dan memberikan rekomendasi pada lima pilar: *cost*, *security*, *reliability*, *operational excellence*, dan *performance*.
2. **Azure Network Watcher** Fitur ini digunakan untuk *monitoring*, *network diagnostics*, dan *traffic visualization*. Sama seperti *Azure Advisor*, fitur ini memenuhi prinsip *"continuous system monitoring and evaluation"* dan *"system log analysis"*. Pemantauan dilakukan berdasarkan *region* dan dapat diakses melalui *CLI*.
3. **Azure VPN Gateway** Digunakan untuk koneksi aman antara jaringan internal Azure dan perangkat eksternal melalui *VPN Point-to-Site (P2S)*. Prinsip yang dipenuhi adalah *"secure line communication"*. Tunnel yang digunakan adalah *IKEv2* dan *OpenVPN (SSL)* dengan metode otentikasi menggunakan *Azure Certificate*.
4. **Azure Application Gateway** Berfungsi sebagai pintu masuk ke *Virtual Machine* (VM) dan *Web Application Firewall* (WAF). Tidak ada *public IP* untuk VM atau *database*, sehingga seluruh koneksi harus melalui *Application Gateway*. Prinsip yang dipenuhi adalah *"secure line communication"*.
5. **Azure Resource Health Monitoring** Fitur ini memberikan status kesehatan VM secara berkala. Prinsip yang dipenuhi adalah *"continuous system monitoring and evaluation"*. Sistem akan mendeteksi dan memberikan peringatan terhadap potensi ancaman atau kegagalan sistem secara proaktif.
6. **Azure Dashboard** Digunakan untuk memantau komponen sistem secara umum. Memenuhi prinsip *"continuous system monitoring and evaluation"* dengan menyediakan

real-time visualization dari status komponen.

7. **Azure Identity and Access Management (IAM)** Digunakan untuk mengatur hak akses pengguna terhadap layanan. IAM memenuhi tiga prinsip terakhir *Zero Trust*: *"time-limited access"*, *"dynamic access policy"*, dan *"evaluated access"*. Pengaturan dilakukan dengan memilih tipe *role assignment* dan durasi akses.

B. Hasil Pengujian Implementasi

Setelah membangun dua infrastruktur, yaitu *Project-Default* (tanpa ZTA) dan *Project-ZTA* (dengan ZTA), pengujian dilakukan untuk menilai penerapan prinsip *Zero Trust*. Hasilnya adalah:

1. **Resources Include Data and Services** Setiap *resource* dianggap entitas mandiri. Dalam pengujian, pemberian akses pada satu *resource* tidak otomatis memberi akses ke *resource* lain berkat *RBAC*.
2. **Secure Communication** Pada *Project-Default*, VM memiliki *public IP* yang bisa diakses langsung. Pada *Project-ZTA*, semua koneksi melalui *VPN Gateway* atau *Application Gateway*.
3. **Access is Time-Limited** Akses diberikan secara terbatas waktu dengan menggunakan pengaturan pada *IAM*, termasuk opsi *Eligible* dan *Time bound*.
4. **Continuous System Monitoring** Monitoring tidak tersedia di *Project-Default*. Sebaliknya, *Project-ZTA* menggunakan *Azure Monitor* dan *Resource Health* untuk deteksi real-time.
5. **Evaluated Access** *IAM* memungkinkan pemberian akses yang sesuai skala (subscription, *resource group*, hingga individual), sesuai dengan prinsip *least privilege*.
6. **System Log Analysis** *Project-ZTA* menggunakan *Activity Log* dan *alert rules* untuk mendeteksi anomali secara otomatis, tidak tersedia di *Project-Default*.

C. Hasil Perbandingan *Microsoft* ZTA dengan Penelitian yang Dilakukan

Panduan resmi *Zero Trust Architecture* dari *Microsoft Azure* mencakup layanan seperti *Azure Firewall*, *DDoS Protection*, *Azure Bastion*, *Key Vault*, dan *Purview* untuk perlindungan menyeluruh. Sebaliknya, implementasi dalam penelitian ini menggunakan pendekatan lebih sederhana dan terfokus pada komponen inti: *Application Gateway* (dengan *WAF v2*), *VPN Gateway*, *Azure Advisor*, dan *Resource Health Monitoring*.

Meskipun lebih sederhana dan *cost-efficient*, pendekatan ini tetap memenuhi ketujuh prinsip *Zero Trust Architecture* dan dapat menjadi solusi bertahap untuk organisasi dengan keterbatasan anggaran, tanpa mengorbankan aspek keamanan sistem *cloud*.

IV. SIMPULAN

Berdasarkan penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa seluruh prinsip dalam *Zero Trust Architecture (ZTA)* berhasil diterapkan secara efektif pada lingkungan *cloud* menggunakan *Microsoft Azure*. Ketujuh prinsip *Zero Trust* yang dirumuskan oleh *NIST*—mulai dari perlindungan terhadap *resource*, komunikasi aman, akses terbatas waktu, kebijakan akses dinamis, pemantauan berkelanjutan, evaluasi akses, hingga analisis *log* sistem—telah diuji dan dibuktikan melalui implementasi nyata pada dua infrastruktur *cloud* yang dibangun, yaitu *Project-Default* dan *Project-ZTA*. Infrastruktur *Project-ZTA* menunjukkan bahwa prinsip-prinsip

tersebut dapat terpenuhi melalui kombinasi layanan seperti *Azure Application Gateway (WAF v2)*, *VPN Gateway*, *Azure IAM*, *Azure Advisor*, dan fitur *monitoring* yang aktif.

Penerapan *Zero Trust* pada *Project-ZTA* juga terbukti mampu menjawab permasalahan yang dipaparkan dalam studi kasus di awal penelitian. Studi kasus pertama mengenai *unauthorized access* di waktu yang tidak semestinya berhasil diminimalkan dengan penerapan akses berbatas waktu dan autentikasi berlapis, yang membatasi waktu serta konteks akses pengguna terhadap *resource*. Sedangkan studi kasus kedua terkait evaluasi akses yang tidak dilakukan dan menyebabkan *eks-karyawan* menyalahgunakan hak akses, dapat diantisipasi melalui fitur *evaluated access* dan *Role-Based Access Control (RBAC)* di *Azure IAM*, yang memungkinkan administrator untuk memantau, membatasi, dan mencabut akses secara selektif dan terkontrol.

Selain itu, hasil perbandingan antara implementasi *ZTA* berdasarkan panduan resmi *Microsoft Azure* dengan implementasi *ZTA* dalam penelitian ini menunjukkan bahwa meskipun panduan *Azure* menawarkan cakupan perlindungan yang lebih komprehensif melalui penggunaan layanan tambahan seperti *Azure Firewall*, *Bastion*, *DDoS Protection*, *Key Vault*, dan *Purview*, pendekatan tersebut memiliki biaya operasional yang relatif lebih tinggi. Di sisi lain, penelitian ini mengusulkan pendekatan *ZTA* yang lebih sederhana dan *cost-efficient* dengan tetap menjaga efektivitas dan kepatuhan terhadap prinsip-prinsip *Zero Trust*. Hal ini menjadikan pendekatan yang digunakan dalam penelitian ini sebagai alternatif yang layak untuk organisasi berskala kecil hingga menengah yang ingin mulai menerapkan *Zero Trust* pada sistem *cloud*-nya tanpa beban biaya yang besar.

DAFTAR RUJUKAN

[1] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[2] P. Borra, "An Overview of Cloud Computing and Leading Cloud Service Providers," *International Journal of Computer Engineering and Technology (IJCET)*, vol. 15, no. 3, pp. 122–133, 2024, doi: 10.17605/OSF.IO/5HQ4M.

[3] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," *IEEE Access*, vol. 9, pp. 20717–20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

[4] R. Kaur and S. Chopra, "Virtualization In Cloud Computing : A Review," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 01–05, Jul. 2020, doi: 10.32628/CSEIT20641.

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[6] B. O. Omoyiola, "An Overview of Root Causes of Cybersecurity Breaches in Organizations," *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4348319.

[7] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, Feb. 2024, doi: 10.9734/JERR/2024/V26I21083.

[8] H. Sharma, "Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security," ESP Journal of Engineering & Technology Advancements. Accessed: Feb. 17, 2025. [Online]. Available: https://www.researchgate.net/publication/383822594_Zero_Trust_in_the_Cloud_Implementing_Zero_Trust_Architecture_for_Enhanced_Cloud_Security

[9] M. Copeland, J. Soh, A. Puca, M. Manning, and D. Gollob, "Microsoft Azure and Cloud Computing," in

Microsoft Azure, Berkeley, CA: Apress, 2015, pp. 3–26. doi: 10.1007/978-1-4842-1043-7_1.

[10] B. Gupta, P. Mittal, and T. Mufti, “A Review on Amazon Web Service (AWS), Microsoft Azure & Google Cloud Platform (GCP) Services,” in *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India*, EAI, 2021. doi: 10.4108/eai.27-2-2020.2303255.

[11] M. A. Vouk, “Cloud Computing - Issues, Research and Implementations,” *Journal of Computing and Information Technology*, vol. 16, no. 4, p. 235, 2008, doi: 10.2498/cit.1001391.

[12] Mjcaparas, “Zero Trust Guidance Center,” https://learn.microsoft.com/en-us/security/zero-trust/.